

**KONSTRUKTION TRANSITIVER
INZIDENZSTRUKTUREN
MIT DIFFERENZENVERFAHREN**

Inaugural-Dissertation
zur
Erlangung der Doktorwürde
des Fachbereichs Mathematik
der Freien Universität Berlin

vorgelegt von
Dieter Jungnickel
aus Berlin

1976

**KONSTRUKTION TRANSITIVER
INZIDENZSTRUKTUREN
MIT DIFFERENZENVERFAHREN**

Inaugural-Dissertation

zur

Erlangung der Doktorwürde
des Fachbereichs Mathematik
der Freien Universität Berlin

vorgelegt von

Dieter Jungnickel
aus Berlin

1. Referent: Prof. Dr. H. Lenz
2. Referent: Prof. Dr. M. Aigner

Tag der mündlichen Prüfung: 25.6.1976



INHALTSVERZEICHNIS

=====

1.	EINLEITUNG	5
2.	PROJEKTIVE KLINGENBERG- UND HJEMSLEVEBENEN	10
2.1	Grundlagen	10
2.2	Differenzenmengen und PK-Ebenen	13
2.3	Reguläre PK-Ebenen	20
2.4	Direkte Konstruktion von H-Matrizen	25
2.5	Kompositionsmethoden zur Konstruktion von H-Matrizen	31
3.	LATEINISCHE QUADRATE UND TD'S	49
3.1	Grundlagen	49
3.2	Differenzenmatrizen und lateinische Quadrate	51
3.3	Differenzenmatrizen und TD's	56
3.4	Konstruktion von Differenzenmatrizen	60
4.	PROJEKTIVE TD-EBENEN	70
4.1	Grundlagen	70
4.2	PTD-Ebenen	72
4.3	Reguläre PTD-Ebenen	76
5.	NORMALE EBENEN UND NTD-EBENEN	83
5.1	Normale Ebenen	83
5.2	Kompositionsmethoden, NTD- und BDTD- Ebenen	88
6.	LITERATURVERZEICHNIS	97



Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41548818_0055

1. EINLEITUNG

=====

Das Ziel dieser Arbeit ist die Konstruktion von endlichen Inzidenzstrukturen, die eine auf den Punkten reguläre und auf den Geraden zumindest semireguläre abelsche Kollineationsgruppe zulassen. Nahegelegt wird diese Fragestellung durch den klassischen Satz von SINGER 1938, der für die desarguesschen projektiven Ebenen eine reguläre zyklische Kollineationsgruppe konstruiert. Wir beschäftigen uns mit Strukturen, für die über die Existenz von regulären Kollineationsgruppen bzw. in vielen Fällen sogar über die Existenz von nichttrivialen Kollineationen überhaupt bisher nichts bekannt ist. Die Existenzfrage für Kollineationen gegebener Strukturen scheint uns ein wesentliches Problem der (endlichen) Geometrie; wir stützen diese Ansicht durch das Urteil zweier der bedeutendsten Mathematiker des letzten Jahrhunderts:

Felix KLEIN (1925, p. 144)

'Als Charakteristikum jeder Geometrie wird ihre Gruppe stets in den Vordergrund der Betrachtung gestellt.'

und

Emil ARTIN (1957, p. 54)

'In modern mathematics the investigation of the symmetries of a given mathematical structure has always yielded the most powerful results.'

Wir werden hauptsächlich Strukturen vom projektiven Typus betrachten; schon CAILEY sagte

'Projective geometry is all geometry.'

(zitiert nach KLEIN 1925, p. 145).

Im zweiten Kapitel beschäftigen wir uns mit projektiven Klingenbergs- und Hjelmslebebenen, von KLINGENBERG 1954, 1955, 1956 eingeführten Verallgemeinerungen der projektiven Ebenen. In derartigen Ebenen sind die Punkt- und

Geradenmenge in 'Nachbarschaftsklassen' zerlegt, die eine gewöhnliche projektive Ebene bilden. Nichtbenachbarte Geraden schneiden sich eindeutig, von benachbarten dagegen wird das nicht verlangt (und dual). Motiviert wird die Untersuchung derartiger Strukturen durch die beim Zeichnen auftretenden 'schleifenden Schnitte'. Wir definieren den Begriff einer 'regulären' Klingenbergebene (im wesentlichen besitzt eine derartige Ebene eine reguläre abelsche Kollineationsgruppe, mit einigen kleinen Zusatzbedingungen), beweisen eine algebraische Bedingung, die für die Existenz regulärer Klingenberg-Ebenen notwendig und hinreichend ist (Abschnitt 2.2) und konstruieren derartige Ebenen mit den Parametern t und r (vgl. Abschnitt 2.1) im Falle $t=q_1 \dots q_n$, q_i Primzahlpotenz und $r \leq q_i$ für $i=1, \dots, n$ (Abschnitt 2.3). Danach konstruieren wir für bestimmte desarguessche Hjelmslebebenen (das sind Klingenbergenebenen mit Zusatzbedingungen, vgl. Abschnitt 2.1) über geeigneten Hjelmslev-Ringen direkt eine reguläre abelsche Kollineationsgruppe (Abschnitt 2.4). Schließlich entwickeln wir Kompositionsmethoden, mit denen aus bekannten regulären Hjelmslebebenen andere mit bisher unbekannten Parametern konstruiert werden können (Abschnitt 2.5). Insbesondere gibt es stets reguläre Hjelmslebebenen mit Parametern (q^n, q) , falls q Primzahlpotenz ist. Falls es reguläre Hjelmslebebenen mit Parametern (s, q) und (r^n, r) gibt, folgt die Existenz von regulären (sr^n, r) -Hjelmslebebenen (insbesondere also von $(q^k r^n, r)$ -Hjelmslebebenen), wenn immer $(r^{n-1} + 1)(r + 1) \leq q + 1 \leq r^n(r + 1)$ gilt. Wir bemerken, daß für Parameter (t, r) , für die t keine Potenz von r ist, bisher überhaupt nichts über die Existenz von Kollineationen bekannt war.

Im dritten Kapitel beschäftigen wir uns mit TDs (transversal designs) und lateinischen Quadraten. Wir fordern wieder reguläre abelsche Automorphismengruppen: für lateinische Quadrate verlangen wir eine auf den Symbolen reguläre Gruppe, für die Anwendung eines Automorphismus mit der Anwendung

einer - für alle Quadrate einer gegebenen orthogonalen Menge gleichen - Zeilenpermutation gleichbedeutend ist. Für TDs verlangen wir eine auf jeder Punktklasse reguläre und auf den Geraden semireguläre Gruppe. Beide Konzepte sind im wesentlichen äquivalent und lassen sich algebraisch durch 'Differenzenmatrizen' beschreiben. Nach der Zusammenstellung der notwendigen Grundlagen (Abschnitt 3.1) wird der Zusammenhang zwischen Differenzenmatrizen und lateinischen Quadraten (Abschnitt 3.2) bzw. TDs (Abschnitt 3.3) untersucht. Dabei ergibt sich auch eine Verbindung zur (p,G) -Transitivität projektiver Ebenen. Schließlich werden Differenzenmatrizen konstruiert (Abschnitt 3.4), teils direkt (z.B. aus elementar-abelschen Gruppen), teils mit Kompositionsmethoden.

Im vierten Kapitel beschäftigen wir uns mit TD-Ebenen, die sich in natürlicher Weise aus dem Studium bestimmter Klassen von Epimorphismen partieller Ebenen ergeben und von LENZ|JUNGNICKEL 1976 eingeführt wurden. Wir stellen zunächst die wichtigsten Definitionen und Resultate zusammen (Abschnitt 4.1), führen dann projektive TD-Ebenen ein und kennzeichnen sie auf eine mehr geometrische Weise (Abschnitt 4.2). Schließlich konstruieren wir projektive TD-Ebenen mit auf den Punkten regulärer und auf den Geraden semiregulärer abelscher Kollineationsgruppe (Abschnitt 4.3); dies erfolgt wieder mit Differenzenmatrizen.

Im fünften, abschließenden Kapitel betrachten wir Verallgemeinerungen, für die die Bildebenen nicht mehr projektive Ebenen sind. Dazu definieren wir zunächst 'normale' Ebenen; derartige Ebenen sind durch eine Verallgemeinerung der gewöhnlichen Differenzenfamilien (wie sie z.B. in elementar-abelschen Gruppen von WILSON 1972 konstruiert wurden) beschreibbar. Wir führen Beispiele von Differenzenfamilien an (Abschnitt 5.1). Danach entwickeln wir Kompositionsmethoden, die u.a. auch bisher nicht bekannte Beispiele gewöhnlicher

Differenzenfamilien und damit Blockpläne mit regulärer Automorphismengruppe für neue Werte von v , die keine Primzahlpotenzen sind, liefern. Ferner konstruieren wir so reguläre TD-Ebenen über normalen Ebenen bzw. Blockplänen (Abschnitt 5.2).

Schließlich folgt ein ausführliches Literaturverzeichnis.

Wir setzen Kenntnis von Inzidenzstrukturen, Blockplänen, projektiven Ebenen, Differenzenfamilien, lateinischen Quadraten, endlichen Körpern etc. voraus. Für den allgemeinen Hintergrund seien besonders die Werke von HALL 1967 und DEMBOWSKI 1968 herausgehoben. Zur projektiven Geometrie vergleiche man ferner ARTIN 1967, HUGHES | PIPER 1968, LENZ 1965, 1975 und PICKERT 1975; zur Kombinatorik DEMBOWSKI 1970, LÜNEBURG 1971 und RYSER 1963; zur Algebra LÜNEBURG 1973 und VAN DER WAERDEN 1971; zur Gruppentheorie HALL 1959; für Differenzenmengen BAUMERT 1971; und für Blockpläne und lateinische Quadrate auch HANANI 1975. Speziellere Literatur ist stets zitiert.

Zur Schreibweise verabreden wir folgendes: Punkte werden stets mit kleinen lateinischen Buchstaben ($p, q, r, \dots$), Geraden stets mit großen lateinischen Buchstaben ($G, H, K, \dots$) bezeichnet; Inzidenzstrukturen mit großen griechischen ($\Sigma, \Pi, \Delta, \dots$) und Abbildungen mit kleinen griechischen Buchstaben ($\pi, \varphi, \psi, \dots$); Punkt- bzw. Geradenmengen mit großen deutschen ($\mathcal{U}, \mathcal{G}, \mathcal{P}, \dots$) und Gruppen ebenfalls mit großen deutschen Buchstaben ($\mathcal{G}, \mathcal{R}, \dots$). $\mathbb{Z}_v$ bezeichnet die Gruppe der ganzen Zahlen mod v und $\text{GF}(q)$ den endlichen Körper der Ordnung q , $\text{GF}(q)^*$ seine multiplikative und $\text{EA}(q)$ seine additive Gruppe. Die Symbole

(p) , $[p]$, $[p,q]$ bzw. (G) , $[G]$, $[G,H]$ sind wie bei DEMBOWSKI 1968 erklärt. Falls Punkte p,q eine eindeutige Verbindungsgerade besitzen, bezeichnen wir sie mit pq ; dual ist $G \cap H$ erklärt. Alle hier untersuchten Inzidenzstrukturen gestatten es, die Geraden als Punktmengen aufzufassen; wir werden daher nicht immer streng zwischen Inzidenzrelation I und Enthaltenseins-Relation $\in$ unterscheiden.

Abschließend möchte ich allen, die mir mit Anregungen und Diskussionen geholfen haben, danken: insbesondere Herrn Prof. Dr. M. Aigner, Herrn Dr. J. Röhmel, Herrn Dr. G. Törner und Herrn A. Neumaier. Ganz besonderen Dank schulde ich meinem verehrten akademischen Lehrer, Herrn Prof. Dr. H. Lenz, für die Betreuung dieser Arbeit und seine stete Hilfsbereitschaft. Schließlich möchte ich es nicht versäumen, mich meines verehrten Schullehrers, des leider all zu früh verstorbenen Oberschulrats Herrn D. Wilken, dankbar zu erinnern; ohne ihn wäre ich sicherlich nicht zur Mathematik gelangt.

2. PROJEKTIVE KLINGENBERG- UND HJELMSLEVEBENEN

In diesem Kapitel konstruieren wir projektive Klingenberg- und Hjelsmslelebenen mit abelscher, auf Punkten und Geraden transitiver (daher regulärer, cf. WIELANDT 1964, Proposition 4.4) Kollineationsgruppe.

2.1 Grundlagen

2.1.1 Definition

Eine projektive Klingenbergebene (kurz: PK-Ebene) Π ist eine Inzidenzstruktur $\Pi = (\mathcal{P}, \mathcal{G}, I)$ zusammen mit einer Äquivalenzrelation $\circ$ auf $\mathcal{P}$ und $\mathcal{G}$ ('Nachbarschaftsrelation'; die Äquivalenzklasse von p bzw. G wird mit p' bzw. G' bezeichnet), für die gilt:

- (PK 1) $p \not\circ q \Rightarrow [p, q] = 1$ für alle $p \in \mathcal{P}$.
- (PK 2) $G \not\circ H \Rightarrow [G, H] = 1$ für alle $G \in \mathcal{G}$.
- (PK 3) Setzt man für $p \in \mathcal{P}$ und $G \in \mathcal{G}$ $p' \perp G'$ genau dann, wenn es $q \in \mathcal{P}$ und $H \in \mathcal{G}$ gibt mit $p \circ q$, $G \circ H$ und $q \perp H$, so bilden die Äquivalenzklassen bezüglich $\circ$ eine projektive Ebene Π' .

Eine projektive Hjelsmsleebene (kurz: PH-Ebene) ist eine PK-Ebene, die außerdem noch erfüllt:

- (PH 1) $p \circ q \Leftrightarrow [p, q] > 1$ für alle $p, q \in \mathcal{P}$.
- (PH 2) $G \circ H \Leftrightarrow [G, H] > 1$ für alle $G, H \in \mathcal{G}$.

2.1.2 Satz

$\Pi = (\mathcal{P}, \mathcal{G}, I)$ sei eine endliche PK-Ebene. Dann gibt es natürliche Zahlen t und r , die Parameter von Π , für die gilt:

- (i) $\text{card } p' = \text{card } G' = t^2$ für alle $p \in \mathcal{P}$ und alle $G \in \mathcal{G}$.
- (ii) Für jede Fahne (p, G) gilt:
 $\text{card } p' \cap (G) = \text{card } G' \cap (p) = t$.

- (iii) r ist die Ordnung von Π' .
- (iv) Falls $t \neq 1$, folgt $r \leq t$. Π heit dann echt.
- (v) $[p] = [G] = t(r+1)$ fr alle $p \in \mathcal{P}$ und alle $G \in \mathcal{G}$.
- (vi) $\text{card } \mathcal{P} = \text{card } \mathcal{G} = t^2(r^2+r+1)$.

Beweis:

KLEINFELD 1959. Man vergleiche auch LNEBURG 1971, DRAKE|LENZ 1976 und JUNGnickel 1975.

2.1.3 Definition

$\mathcal{E}\mathcal{G}$ bezeichne das Spektrum aller Paare (t, r) , die als Parameter einer PH-Ebene auftreten, und $\mathcal{E}\mathcal{R}$ die analoge Menge fr PK-Ebenen.

2.1.4 Satz

- (i) $(1, r) \in \mathcal{E}\mathcal{G} \Rightarrow (r^n, r) \in \mathcal{E}\mathcal{G}$ fr jedes $n \in \mathbb{N}$.
Insbesondere gilt stets $(q^n, q) \in \mathcal{E}\mathcal{G}$, wenn q Primzahlpotenz ist.
- (ii) $(t, r) \in \mathcal{E}\mathcal{R} \Leftrightarrow (1, r) \in \mathcal{E}\mathcal{R} \wedge N(t) \geq r-1$.
Dabei bezeichnet $N(t)$ die Maximalzahl paarweise orthogonaler lateinischer Quadrate der Ordnung t .

Beweis:

- (i) ARTMANN 1971.
- (ii) DRAKE|LENZ 1976.

Bis 1974 war ber die Existenz von PH-Ebenen **nichts** weiter bekannt. Dann gelang es DRAKE|LENZ 1976 unendlich viele Serien weiterer Elemente von $\mathcal{E}\mathcal{G}$ zu konstruieren:

2.1.5 Satz

- (i) Ist $(t, r) \in \mathcal{E}\mathcal{G}$ und ist $q := t(r+1)-1$ eine Primzahlpotenz und $(s, q) \in \mathcal{E}\mathcal{G}$, so ist auch $(st, r) \in \mathcal{E}\mathcal{G}$; insbesondere ist stets $(q^n t, r) \in \mathcal{E}\mathcal{G}$.
- (ii) Ist $2(r+1) \leq q+1 \leq r(r+1)$, ist $(1, r) \in \mathcal{E}\mathcal{R}$, ist q Primzahlpotenz und $(s, q) \in \mathcal{E}\mathcal{G}$, so ist auch

- $(sr, r) \in \mathcal{E}_b$, insbesondere $(q^n r, r) \in \mathcal{E}_b$.
- (iii) Sind q, r Primzahlpotenzen mit

$$\left(\sum_{j=0}^b r^j \right) (r+1) \leq q+1 \leq r^{2b} (r+1)$$
 und ist $(s, q) \in \mathcal{E}_b$, so ist auch $(r^{2b} s, r) \in \mathcal{E}_b$.
- (iv) Sind q, r Primzahlpotenzen mit

$$\left(r^b + \sum_{j=0}^b r^j \right) (r+1) \leq q+1 \leq r^{2b+1} (r+1)$$
 und ist $(s, q) \in \mathcal{E}_b$, so ist auch
 $(r^{2b+1} s, r) \in \mathcal{E}_b$.

Beweis:

(i) und (ii): DRAKE|LENZ 1976.

(iii) und (iv): DRAKE 1975.

Weiter ist über $\mathcal{E}_b$ nichts bekannt.

2.1.6 Definition

$\Pi = (\mathcal{P}, \mathcal{B}, I)$ sei eine PK-Ebene und $\varphi: \mathcal{P} \cup \mathcal{B} \rightarrow \mathcal{P} \cup \mathcal{B}$ eine bi-jektive Abbildung mit

- (i) $\varphi(\mathcal{P}) = \mathcal{P}$ und $\varphi(\mathcal{B}) = \mathcal{B}$.
- (ii) $pIG \Leftrightarrow p^{\varphi} I G^{\varphi}$ für alle $p \in \mathcal{P}$ und alle $G \in \mathcal{B}$.
- (iii) $pq \Leftrightarrow p^{\varphi} q^{\varphi}$ für alle $p, q \in \mathcal{P}$.
- (iv) $G \circ H \Leftrightarrow G^{\varphi} \circ H^{\varphi}$ für alle $G, H \in \mathcal{B}$.

Dann heißt φ eine Kollineation von Π .

Man beachte, daß für PH-Ebenen die Bedingungen (iii) und (iv) aufgrund der Bijektivität und (i) und (ii) bereits wegen (PH 1) und (PH 2) folgen; ob das auch für PK-Ebenen gilt, ist ungeklärt.

Für Parameterpaare (t, r) , wo t keine Potenz von r ist, ist bisher nichts über die Existenz nichttrivialer Kollineationen bekannt; und auch in den übrigen Fällen, für die man Beispiele über lokalen Ringen kennt (vgl. KLINGENBERG 1954, 1955, 1956) weiß man nichts über die Existenz regulärer Kollineationsgruppen. Diesem Problem werden wir uns

jetzt zuwenden. Zuvor seien noch als allgemeine Literaturhinweise über PK- und PH-Ebenen DEMBOWSKI 1967 und JUNGnickel 1975 erwähnt. Schließlich wollen wir noch darauf hinweisen, daß die hier betrachteten Strukturen nichts mit Hjelmslebebenen über Hjelmslevgruppen im Sinne von BACHMANN 1973 zu tun haben.

2.2 Differenzenmengen und PK-Ebenen

2.2.1 Definition

$\Pi = (\mathfrak{P}, \mathfrak{G}, I)$ sei eine PK-Ebene. Π heißt regulär, wenn es eine abelsche Kollineationsgruppe $\mathfrak{G}$ von Π gibt mit:

$$(2.1) \quad \mathfrak{G} = \mathfrak{g} \oplus \mathfrak{n}.$$

(2.2) $\mathfrak{n}$ bildet jede Punktklasse p' und jede Geradenklasse G' regulär auf sich ab.

(2.3) $\mathfrak{G}$ ist auf $\mathfrak{P}$ und $\mathfrak{G}$ regulär.

$\mathfrak{g}$ operiert dann offenbar auf den Punkten und Geraden von Π' regulär. In den bekannten Fällen ist $\mathfrak{g}$ dann eine zyklische Gruppe $\mathbb{Z}_v$ mit $v := r^2 + r + 1$ und r Primzahlpotenz.

2.2.2 Definition

$\mathfrak{R}$ bezeichne das Spektrum der Paare (t, r) , für die eine reguläre PK-Ebene existiert; $\mathfrak{R}_H$ die analoge Menge für PH-Ebenen.

2.2.3 Definition

$\mathfrak{g}$ sei eine abelsche Gruppe der Ordnung $v := r^2 + r + 1$, $\mathfrak{n}$ eine abelsche Gruppe der Ordnung t^2 und $\mathfrak{G} := \mathfrak{g} \oplus \mathfrak{n}$. Dann heißt

$$(2.4) \quad D := \{(a_i, a_{ij}) : i=0, \dots, r; j=1, \dots, t\} \subseteq \mathfrak{G}$$

eine (t, r) -Differenzenmenge, falls gilt:

(2.5) Unter den Differenzen

$$(a_i, a_{ik}) - (a_j, a_{jl}) \quad \text{mit } i \neq j, i, j = 0, \dots, r \text{ und}$$

$k, l = 1, \dots, t$ kommt jedes der $r(r+1)t^2$ Elemente (x, y) von $\mathfrak{G}$ mit $x \neq 0$ genau einmal vor.

D heißt speziell, falls zusätzlich gilt:

- (2.6) Unter den $(r+1)t(t-1)$ Differenzen
 $(a_i, a_{ij}) - (a_i, a_{ik})$ mit $j \neq k$, $i=0, \dots, r$ und
 $j, k = 1, \dots, t$ kommt jedes Element der Form $(0, x)$
 von $\mathfrak{G}$ mindestens zweimal vor.

2.2.4 Beispiel

$t=r=2$, $\mathfrak{g} = \mathbb{Z}_7$, $\mathfrak{H} = \text{GF}(4)$ mit erzeugendem Element w von $\text{GF}(4)^*$. Wir setzen

$D := \{(1,0), (1,1), (2,0), (2,w), (4,0), (4,w^2)\}$
 und erhalten eine $(2,2)$ -Differenzenmenge.

2.2.5 Definition

Es sei $\Delta = (\mathfrak{p}, \mathfrak{g}, I)$ eine beliebige Inzidenzstruktur und $\circ$ eine Äquivalenzrelation auf $\mathfrak{p}$. Wir definieren eine Relation $\circ'$ auf $\mathfrak{g}$ durch

- (2.7) $G \circ' H$ dann und nur dann, wenn es für jeden Punkt p auf einer der Geraden G, H einen Punkt α auf der anderen der beiden Geraden gibt mit
 $p \circ \alpha$.

Offenbar ist auch $\circ'$ eine Äquivalenzrelation. $\circ'$ heißt die von $\circ$ auf $\mathfrak{g}$ erzeugte Äquivalenzrelation. Meistens schreiben wir einfach wieder $\circ$ statt $\circ'$.

2.2.6 Satz

D sei eine (t, r) -Differenzenmenge über $\mathfrak{G} = \mathfrak{g} \oplus \mathfrak{H}$. Dann ist die Inzidenzstruktur $\Pi(D) = (\mathfrak{G}, \mathfrak{g}(D), \epsilon)$ mit

$$(2.8) \quad \mathfrak{g}(D) := \{D+x: x \in \mathfrak{G}\}$$

eine bezüglich $\mathfrak{G}$ reguläre PK-Ebene. Ist D speziell, so ist $\Gamma(D)$ sogar PH-Ebene. Π hat die Parameter (t, r) .

Ist umgekehrt Π eine bezüglich $\mathfrak{G}$ reguläre (t, r) -PK-Ebene, so gibt es über $\mathfrak{G}$ eine (t, r) -Differenzenmenge D mit

$\Pi \approx \Pi(D)$. D ist speziell, falls Π PH-Ebene ist.

Beweis:

' $\Rightarrow$ '

D sei also (t,r) -Differenzenmenge über $\mathfrak{G}$. Wir definieren eine Äquivalenzrelation $\circ$ auf den Punkten von $\Pi(D)$ durch

$$(2.9) \quad (x,y) \circ (x',y') \Leftrightarrow x=x'$$

und bezeichnen wieder mit $\circ$ die erzeugte Äquivalenzrelation auf $\Pi(D)$ (2.2.5). Da D eine Differenzenmenge ist, ist

$D' := \{a_0, \dots, a_r\}$ eine gewöhnliche Differenzenmenge in $\mathfrak{g}$

(D sei wie in (2.4) dargestellt). Daher bilden die Elemente von $\mathfrak{g}$ als Punkte und die Mengen $D'+x$ mit $x \in \mathfrak{g}$ als Geraden

eine projektive Ebene $\Pi'(D)$ der Ordnung r . Offenbar ist

die Abbildung $\varphi: \Pi(D) \rightarrow \Pi'(D)$ mit $(x,y) \mapsto x$ ein Epimorphismus; ferner gilt poq bzw. GoH offensichtlich genau

dann, wenn $p\varphi=q\varphi$ bzw. $G\varphi=H\varphi$ gilt. $\Pi(D)$ erfüllt also (PK 3).

Es bleibt die Gültigkeit von (PK 1) und (PK 2) nachzuweisen.

Zunächst sei $(x,y) \not\phi (x',y')$, also $x-x' \neq 0$. Nach

(2.5) gilt für geeignete Indizes i,j,k,l mit $i \neq j$

$(x-x',y-y') = (a_i, a_{ik}) - (a_j, a_{jl})$. Dann folgt:

$$(x,y) = (a_i, a_{ik}) + (x-a_i, y-a_{ik}) \in D+(x-a_i, y-a_{ik})$$

und

$$(x',y') = (x-a_i+a_j, y-a_{ik}+a_{jl}) = (a_j, a_{jl}) + (x-a_i, y-a_{ik})$$

$$\in D+(x-a_i, y-a_{ik}).$$

(x,y) und (x',y') sind also verbindbar. Sei nun etwa $(x,y),$

$(x',y') \in D+(u,v)$, d.h. $(x,y) = (a_i, +u, a_{ik}, +v)$ und

$(x',y') = (a_j, +u, a_{jl}, +v)$ für geeignete Indizes $i',k',j',$

l' . Dann folgt $u = x-a_i = x'-a_{j'}$, und $v = y-a_{ik} =$

$y'-a_{j'l'}$, also $(x-x',y-y') = (a_i, a_{ik}) - (a_{j'}, a_{j'l'})$.

Wegen (2.5) muß dann $i=i', j=j', k=k', l=l'$ und damit

$u = x-a_i$ und $v = y-a_{ik}$ gelten, d.h. (x,y) und (x',v') sind

eindeutig verbindbar. Also erfüllt $\Pi(D)$ (PK 1).

Es sei nun $D+(x,y) \not\phi D+(x',v')$, d.h. $x \neq x'$. Nach (2.5) gibt

es Indizes i,j,k,l mit $(x-x',y-y') = (a_i, a_{ik}) - (a_j, a_{jl})$.

Dann gilt

$$(a_{j+x}, a_{j_l+y}) \in D+(x, y)$$

und

$$(a_{j+x}, a_{j_l+y}) = (a_{i+x'}, a_{i_k+y'}) \in D+(x', y').$$

Sei umgekehrt etwa $(u, v) \in D+(x, y)$, $D+(x', y')$. Dann gilt $(u, v) = (a_{j+x}, a_{j_l+y}) = (a_{i+x'}, a_{i_k+y'})$ für geeignete Indizes i', j', k', l' . Es folgt $(x-x', y-y') = (a_{i_l}, a_{i_k}) - (a_{j_l}, a_{j_l})$ und daher wegen (2.5) $i=i', j=j', k=k', l=l'$ und somit $u = a_{j+x}$ und $v = a_{j_l+y}$. Daher erfüllt $\Pi(D)$ auch (PK 2).

$\Pi(D)$ ist also eine PK-Ebene, die nach 2.1.2 offenbar die Parameter t und r besitzt. Die Translationen τ_{xy} mit $\tau_{xy} : (a, b) \mapsto (a+x, b+y)$ mit $(x, y) \in \mathcal{G}$ bilden offenbar eine zu $\mathcal{G}$ isomorphe Kollineationsgruppe von $\Pi(D)$, bezüglich der $\Pi(D)$ regulär ist: (2.1) und (2.3) sind offenbar erfüllt und (2.2) gilt nach (2.8) und (2.7).

Sei nun D sogar eine spezielle Differenzenmenge. Es bleibt zu zeigen, daß $\Pi(D)$ (PH 1) und (PH 2) erfüllt. Seien also verschiedene Nachbarpunkte, etwa (x, y) und (x', y') mit $y \neq y'$ gegeben. Nach (2.6) ist die Differenz $(0, y-y')$ mindestens zweimal darstellbar, etwa $(0, y-y') = (a_i, a_{ij}) - (a_i, a_{ik}) = (a_1, a_{1m}) - (a_1, a_{1n})$ für geeignete Indizes i, j, k, l, m, n mit $j \neq k$, $m \neq n$ und $(i, j) \neq (1, m)$. Wie oben folgt

$$(x, y), (x', y') \in D+(x-a_i, y-a_{ij}), D+(x-a_1, y-a_{1m}),$$

d.h., (x, y) und (x', y') liegen auf mindestens zwei verschiedenen Geraden. Umgekehrt sind mehrfach verbindbare Punkte nach (PK 1) benachbart. Also gilt (PH 1).

Seien nun zwei verschiedene Nachbargeraden gegeben, etwa $D+(u, v)$ und $D+(u, w)$ mit $v \neq w$. Nach (2.6) gibt es Indizes i, j, k, l, m, n mit $j \neq k$, $m \neq n$ und $(i, j) \neq (1, m)$, so daß gilt:

$$(0, w-v) = (a_i, a_{ij}) - (a_i, a_{ik}) = (a_1, a_{1m}) - (a_1, a_{1n}).$$

Wie oben folgt

$$(a_i+u, a_{ij}+v), (a_1+u, a_{1m}+v) \in D+(u, v), D+(u, w).$$

Umgekehrt sind Geraden mit mindestens zwei Schnittpunkten

nach (PK 2) benachbart.

$\Pi(D)$ erfüllt somit auch (PH 2), ist also eine PH-Ebene.

' $\Leftarrow$ '

Sei nun Π eine bezüglich $\mathfrak{G}$ reguläre (t,r) -PK-Ebene. Wir wählen einen willkürlichen Basispunkt $(0,0)$. Dann erhält der Punkt p die Koordinaten $(x,y) \in \mathfrak{G}$, falls Anwendung von (x,y) auf $(0,0)$ p ergibt. Nach (2.3) ist das wohldefiniert. Nach (2.2) sind (x,y) und (x',y') genau dann benachbart, wenn $x=x'$ gilt. Wir wählen nun eine feste Basisgerade, etwa D (wie in (2.4) beschrieben). Jede Gerade von Π ist dann nach (2.3) eindeutig in der Form $D+(x,y)$ mit $(x,y) \in \mathfrak{G}$ darstellbar. Umgekehrt stellen (x,y) bzw. $D+(x,y)$ auch stets wirklich einen Punkt bzw. eine Gerade von Π dar.

Wir behaupten, daß D eine (t,r) -Differenzenmenge über $\mathfrak{G}$ ist. Es sei $x \neq 0$, $x \in \mathfrak{G}$. Nach (PK 1) sind dann die Punkte $(0,0)$ und (x,y) eindeutig verbindbar, etwa durch $D+(u,v)$. Dann gibt es Indizes i,j,k,l mit $i \neq j$ und $(x,y) = (a_i, a_{ij}) + (u,v)$, $(0,0) = (a_k, a_{kl}) + (u,v)$. Dann folgt

$$u = x - a_i = -a_k \quad \text{und} \quad v = y - a_{ij} = -a_{kl}, \text{ d.h.} \\ (x,y) = (a_i - a_k, a_{ij} - a_{kl}).$$

Umgekehrt würde aus der Existenz einer weiteren derartigen Darstellung von (x,y) die Existenz einer weiteren Verbindungsgeraden von (x,y) und $(0,0)$ folgen, wie oben gezeigt; dies wäre ein Widerspruch zu (PK 1). Also erfüllt D (2.5).

Es ist offensichtlich, daß $\Pi \cong \Pi(D)$ gilt.

Sei jetzt Π sogar PH-Ebene. Die Nachbarpunkte $(0,0)$ und $(0,y)$ ($y \neq 0$, $y \in \mathfrak{M}$) sind dann nach (PH 1) auf mindestens zwei verschiedenen Geraden, etwa $D+(x,u)$ und $D+(x,v)$. Es sei etwa $(0,0) = (a_i, a_{ij}) + (x,u) = (a_i, a_{ik}) + (x,v)$ und $(0,y) = (a_i, a_{ih}) + (x,u) = (a_i, a_{il}) + (x,v)$. Dann folgt

$$(0,y) = (a_i, a_{ih}) - (a_i, a_{ij}) = (a_i, a_{il}) - (a_i, a_{ik}), \\ \text{d.h. } D \text{ ist speziell.}$$

Damit ist der Beweis des Satzes vollständig.

2.2.7 Zusatz

D sei eine Differenzenmenge. Falls für ein $y \neq 0$, $y \in \mathfrak{M}$ gilt

$$(0, y) = (a_i, a_{ij}) - (a_i, a_{ik}) = (a_1, a_{1m}) - (a_1, a_{1n}),$$

so folgt $i=1$.

Beweis:

Sonst wären nämlich die nichtbenachbarten Punkte $(a_i, a_{ik}+y)$ und $(a_1, a_{1n}+y)$ von $\Pi(D)$ Schnittpunkte der Geraden D und $D+(0, y)$, im Widerspruch zu (PK 1) und 2.2.6.

2.2.8 Definition

$\mathfrak{T}$ sei eine abelsche Gruppe der Ordnung t^2 und $A := (a_{ik})$ mit $i=0, \dots, r$, $k=1, \dots, t$ und $a_{ik} \in \mathfrak{M}$ eine $(r+1) \times t$ -Matrix.

A heißt eine (t,r)-Klingenberg-Matrix (kurz: (t,r)-K-Matrix), falls gilt:

$$(2.9) \quad \text{Für jedes Paar } (i, j) \text{ mit } i \neq j \text{ und } i, j = 0, \dots, r \\ \text{gilt } \mathfrak{M} = \{a_{ik} - a_{jl} : k, l = 1, \dots, t\}.$$

Gilt überdies noch

$$(2.10) \quad \text{Unter den } (r+1)t(t-1) \text{ Differenzen } a_{ik} - a_{il} \text{ mit} \\ i=0, \dots, r, \quad k, l = 1, \dots, t \text{ und } k \neq l \text{ tritt jedes} \\ x \in \mathfrak{M} \text{ mit } x \neq 0 \text{ mindestens zweimal auf.}$$

so heißt A eine (t,r)-Hjelmslev-Matrix (kurz: (t,r)-H-Matrix).

2.2.9 Hilfssatz

Sei D (wie in (2.4) beschrieben) eine (t,r)-Differenzenmenge über $\mathfrak{G} = \mathfrak{g} \oplus \mathfrak{T}$. Dann ist $A := (a_{ik})$ ($i=0, \dots, r$; $k=1, \dots, t$) eine (t,r)-K-Matrix über $\mathfrak{M}$. A ist H-Matrix, falls D speziell ist.

Ist umgekehrt $A = (a_{ik})$ eine (t,r)-K-Matrix über $\mathfrak{M}$ und $D' := \{a_0, \dots, a_r\}$ eine gewöhnliche Differenzenmenge über $\mathfrak{g}$, so ist das nach (2.4) erklärte D eine (t,r)-Differenzenmenge über $\mathfrak{g} \oplus \mathfrak{T}$. D ist speziell, falls A H-Matrix ist.

Beweis:

Offensichtlich, da sich (2.9) und (2.5) bzw. (2.10) und

(2.6) entsprechen.

2.2.10 Korollar

r sei Primzahlpotenz. Dann gilt $(t,r) \in \mathbb{R}\mathbb{R}$ bzw. $(t,r) \in \mathbb{R}\mathbb{S}$ genau dann, wenn eine (t,r) - $\mathbb{K}$ -Matrix bzw. eine (t,r) - $\mathbb{H}$ -Matrix existiert.

Beweis:

Nach dem Satz von SINGER 1938 existiert nämlich stets eine gewöhnliche Differenzenmenge in $\mathbb{Z}_v$ (mit $v := r^2+r+1$), vgl. auch etwa HALL 1967. Die Behauptung folgt daher aus 2.2.6 und 2.2.9.

2.2.11 Hilfssatz

Es sei A eine (t,r) - $\mathbb{K}$ -Matrix über $\mathbb{K}$. A' gehe aus A durch Operationen der folgenden Typen hervor:

- (i) Permutationen innerhalb der Zeilen von A
- (ii) Zeilenpermutationen
- (iii) Addition eines festen $n \in \mathbb{K}$ in einer Zeile von A .

Dann ist auch A' eine $\mathbb{K}$ -Matrix.

Zu jeder $\mathbb{K}$ -Matrix A gibt es daher eine durch Operationen der Typen (i) bis (iii) aus A erhältliche $\mathbb{K}$ -Matrix $B = (b_{ik})$ mit

$$(2.11) \quad b_{0t} = b_{1t} = \dots = b_{rt} = 0$$

$$(2.12) \quad \text{Alle Elemente von } \mathbb{K}, \text{ die nicht in der letzten Spalte auftreten, sind paarweise verschieden und } \neq 0.$$

Ferner gilt $r \leq t$.

Beweis:

Offensichtlich.

2.2.12 Beispiele

Man vergleiche zu den folgenden Beispielen Satz 2.3.1.

$$t=r=2, \mathfrak{N} = \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

$$\begin{pmatrix} (1,1) & (0,0) \\ (1,0) & (0,0) \\ (0,1) & (0,0) \end{pmatrix}$$

$$t=r=3, \mathfrak{N} = \mathbb{Z}_3 \oplus \mathbb{Z}_3$$

$$\begin{pmatrix} (2,2) & (1,1) & (0,0) \\ (2,1) & (1,2) & (0,0) \\ (2,0) & (1,0) & (0,0) \\ (0,2) & (0,1) & (0,0) \end{pmatrix}$$

$$t=r=4, \mathfrak{N} = \text{EA}(4) \oplus \text{EA}(4), w \text{ erzeugendes Element von } \text{GF}(4)^*$$

$$\begin{pmatrix} (w,w) & (w^2,w^2) & (1,1) & (0,0) \\ (w,w^2) & (w^2,1) & (1,w) & (0,0) \\ (w,1) & (w^2,w) & (1,w^2) & (0,0) \\ (w,0) & (w^2,0) & (1,0) & (0,0) \\ (0,w) & (0,w^2) & (0,1) & (0,0) \end{pmatrix}$$

Man bestätigt, daß alle diese Matrizen sogar H-Matrizen sind. (Vgl. 2.4.2).

2.3 Reguläre PK-Ebenen

2.3.1 Satz

t sei Primzahlpotenz und $r \nmid t$. Dann existiert eine (t,r) -K-Matrix über $\text{EA}(t^2)$.

Beweis:

Es sei $F := \text{GF}(t)$ und F^* erzeugt von w . Wir setzen $\mathfrak{N} := F \oplus F = \text{EA}(t^2)$ und definieren die $r+1 \times t$ -Matrix $A = (a_{ik})$ durch

$$a_{ik} := \begin{cases} (0,0) & \text{für } k=t \\ (w^k, 0) & \text{für } k \nmid t \text{ und } i=r-1 \\ (0, w^k) & \text{für } k \nmid t \text{ und } i=r \\ (w^k, w^{i+k}) & \text{sonst} \end{cases}$$

($i=0, \dots, r$; $k=1, \dots, t$), d.h. also

$$A = \begin{pmatrix} (w^1, w^1) & (w^2, w^2) & \dots & (w^{t-1}, w^{t-1}) & (0,0) \\ \vdots & & & & \vdots \\ (w^1, w^{r-1}) & (w^2, w^r) & \dots & (w^{t-1}, w^{t+r-3}) & (0,0) \\ (w^1, 0) & (w^2, 0) & \dots & (w^{t-1}, 0) & (0,0) \\ (0, w^1) & (0, w^2) & \dots & (0, w^{t-1}) & (0,0) \end{pmatrix}$$

Wir behaupten, daß A eine K -Matrix ist.

Betrachten wir zunächst die Differenzen aus den Zeilen r und i ($i \neq r, r-1$). Offenbar ergibt sich jede Differenz der Form $(0, y)$ genau einmal, nämlich als $(0, 0) - (0, 0)$ bzw. als $(0, w^j) - (0, 0)$. Jede Differenz der Form (w^k, y) ergibt sich bei den Elementen $(0, 0) - (w^1, w^{i+1})$ bzw. $(0, w^j) - (w^1, w^{i+1})$ ($j=1, \dots, t-1$; $w^1 := -w^k$), da natürlich gilt $F \cdot w^{i+1} = F$. Analog verfährt man bei den Differenzen, die sich aus den Zeilen r und $r-1$ bzw. aus den Zeilen i und $r-1$ ($i \neq r, r-1$) ergeben (im letzten Fall benutzt man Fallunterscheidung nach den zweiten - statt der ersten - Koordinaten der Differenzen).

Es bleiben die Differenzen von Zeilen i und j mit $i \neq j$ und $i, j \neq r, r-1$ zu untersuchen. Die Differenzen mit erster Koordinate 0 sind

$$\begin{aligned} & \{(w^1, w^{i+1}) - (w^1, w^{j+1}), \dots, (w^{t-1}, w^{i+t-1}) - (w^{t-1}, w^{j+t-1}), \\ & (0, 0) - (0, 0)\} \\ & = \{(0, x(w^i - w^j)) : x=0, w^1, \dots, w^{t-1}\}, \end{aligned}$$

wegen $w^i - w^j \neq 0$ also alle Elemente der Form $(0, y)$.

Sei nun $x \neq 0$, etwa $x = w^k$. Wir behaupten, daß die Differenzen mit erster Koordinate x gerade als Elemente der Form

$$(2.13) \quad (x, w^j(y(w^{i-j-1}) + x)) \quad \text{mit } y \in F$$

auftreten, was wegen $i \neq j$ alle Elemente der Form (x, z) ergibt.

Zunächst ist die Differenz zu $(0, 0)$

$$(w^k, w^{k+i}) - (0, 0) = (x, w^j(x(w^{i-j-1}) + x)),$$

hat also die Form (2.13) mit $y=x$. Die Differenz von $(0, 0)$ aus ist, falls wir $-x =: w^{k'}$ setzen,

$$(0, 0) - (w^{k'}, w^{k'+j}) = (w^k, w^{k+j}) = (x, w^j(0(w^{i-j-1}) + x)),$$

hat also die Form (2.13) für $y=0$.

Ist schließlich $y \neq 0, x$, etwa $y = w^l$ mit $l \neq k$, so gibt es genau ein $m \in \{0, \dots, t-1\} \setminus \{1\}$ mit $x = w^k = w^l - w^m$. Es folgt

$$\begin{aligned} & (w^1, w^{1+i}) - (w^m, w^{m+j}) = (x, w^j(w^{i-j+1} - w^n)) \\ & = (x, w^j(w^1(w^{i-j-1}) + w^1 - w^m)) = (x, w^j(y(w^{i-j-1}) + x)). \end{aligned}$$

Also tritt tatsächlich jedes Element mit erster Koordinate x auf; A ist also eine K -Matrix.

2.3.2 Satz

Falls eine (t,r) -K-Matrix über $\mathfrak{M}$ und eine (t',r) -K-Matrix über $\mathfrak{M}'$ existieren, so existiert auch eine (tt',r) -K-Matrix über $\mathfrak{M} \oplus \mathfrak{M}'$.

Beweis:

Es sei $A = (a_{ik})$ ($i=0,\dots,r$; $k=1,\dots,t$) eine (t,r) -K-Matrix über $\mathfrak{M}$ und $B = (b_{ik})$ ($i=0,\dots,r$; $k=1,\dots,t'$) eine (t',r) -K-Matrix über $\mathfrak{M}'$. Wir definieren über $\mathfrak{M} \oplus \mathfrak{M}'$ eine Matrix $C := (c_{ik})$ mit $i=0,\dots,r$ und $k=1,\dots,tt'$ durch

$$c_{ik} := (a_{i, \alpha k}, b_{i, k-(\alpha k-1)t'}),$$

wobei αk die kleinste ganze Zahl $\geq \frac{k}{t'}$ bezeichnet. Wir erhalten also

$$C = \begin{pmatrix} (a_{01}, b_{01}) \dots (a_{01}, b_{0t'}) \dots (a_{0t}, b_{01}) \dots (a_{0t}, b_{0t'}) \\ \vdots \\ (a_{r1}, b_{r1}) \dots (a_{r1}, b_{rt'}) \dots (a_{rt}, b_{r1}) \dots (a_{rt}, b_{rt'}) \end{pmatrix}$$

Sei nun ein Paar (i,j) mit $i \neq j$ und $i, j = 0, \dots, r$ fest gewählt. Wir müssen die Gültigkeit von (2.9) für C nachweisen. Ist x als erste Koordinate vorgegeben, so erscheint x als genau eine Differenz $a_{ik} - a_{jl}$, da A eine K-Matrix ist. Ist y als zweite Koordinate gegeben, so erscheint y genau einmal in der Form $b_{ik} - b_{jl}$, da B eine K-Matrix ist. Nach Konstruktion von C enthalten die i -te bzw. j -te Zeile die Paare (a_{ik}, b_{ik}) bzw. (b_{jl}, b_{jl}) genau einmal. Daher ergibt sich jede mögliche Differenz (x,y) genau einmal aus den Differenzen der Zeilen i und j .

2.3.3 Korollar

Es sei $t=q_1 \dots q_n$ die Primzahlpotenzzerlegung von t . Ist dann $r \leq q_i$ für $i=1, \dots, n$, so gibt es eine (t,r) -K-Matrix über $EA(q_1^2) \oplus \dots \oplus EA(q_n^2)$.

2.3.4 Korollar

Es sei $t = q_1 \dots q_n$ die Primzahlpotenzzerlegung von t . Ist dann $r \leq q_i$ für $i=1, \dots, n$ und r Primzahlpotenz, so gilt $(t, r) \in \mathcal{R}\mathcal{R}$.

2.3.5 Satz

Es sei $t = p^n$ Primzahlpotenz und $r \leq p$. Dann gibt es eine (t, r) - K -Matrix über $\mathbb{Z}_t \oplus \mathbb{Z}_t$.

Beweis:

Wir definieren die $r+1 \times t$ -Matrix $A = (a_{ik})$ durch

$$a_{ik} := \begin{cases} (0, 0) & \text{für } k=t \\ (k, 0) & \text{für } k \nmid t \text{ und } i=r-1 \\ (0, k) & \text{für } k \nmid t \text{ und } i=r \\ (k, (i+1)k) & \text{sonst} \end{cases}$$

($i=0, \dots, r$; $k=1, \dots, t$), d.h. wir erhalten

$$A = \begin{pmatrix} (1, 1) & (2, 2) & \dots & (t-1, t-1) & (0, 0) \\ (1, 2) & (2, 4) & \dots & (t-1, 2(t-1)) & (0, 0) \\ \vdots & & & & \vdots \\ (1, r-1) & (2, 2r-2) & \dots & (t-1, (r-1)(t-1)) & (0, 0) \\ (1, 0) & (2, 0) & \dots & (t-1, 0) & (0, 0) \\ (0, 1) & (0, 2) & \dots & (0, t-1) & (0, 0) \end{pmatrix}$$

Der Nachweis, daß A tatsächlich eine K -Matrix ist, wird ähnlich wie der Beweis von 2.3.1 geführt; man beachte dabei, daß $1, \dots, p-1$ und $i-j$ für $i \nmid j$ und $i, j = 0, \dots, r-1$ zu t relativ prim, also in $\mathbb{Z}_t$ invertierbar sind.

Wir weisen darauf hin, daß der Fall $n=1$ bereits durch Satz 2.3.1 erledigt war.

Schließlich geben wir noch einige weitere Automorphismen der so konstruierten PK-Ebenen an:

2.3.6 Satz

t und r seien Primzahlpotenzen mit $r \nmid t$. Die (t, r) -K-Matrix A sei wie in 2.3.1 konstruiert. Π sei eine gemäß 2.2.6 und 2.2.9 konstruierte, bezüglich $\mathfrak{G} := \mathfrak{g} \oplus \text{EA}(t^2)$ reguläre PK-Ebene. Dann läßt Π eine Kollineationsgruppe $\mathfrak{H} \cong \mathbb{Z}_{t-1}$ zu, die auf Π' die Identität induziert. Die von $\mathfrak{G}$ und $\mathfrak{H}$ erzeugte Kollineationsgruppe $\mathfrak{U}$ von Π ist das semidirekte Produkt von $\mathfrak{G}$ mit $\mathfrak{H}$. $\mathfrak{U}$ ist nicht abelsch.

Beweis:

Wir setzen $\mathfrak{H} := \{\pi_i : i=0, \dots, t-2\}$ mit

$$(2.14) \quad \pi_i : (a, x, y) \mapsto (a, xw^i, yw^i) \quad (a \in \mathfrak{g}, x, y \in \text{EA}(t)).$$

Da jedem π_i eine Spaltenpermutation von A entspricht, ist π_i nach 2.2.9 und 2.2.6 tatsächlich eine Kollineation von Π ; π_i läßt nämlich die Startgerade D fest und überführt die Geraden $D+(x, y, z)$ daher in $D+(x, yw^i, zw^i)$. Offenbar gilt $\mathfrak{H} \cong \mathbb{Z}_{t-1}$. Wegen (2.9) induziert jedes π_i auf Π' die identische Kollineation.

Es gilt offenbar $\mathfrak{G} \cap \mathfrak{H} = 1$. Nach Definition sind $\mathfrak{H}$ und $\mathfrak{G}$ Untergruppen von $\mathfrak{U}$. Bezeichnen wir die Kollineation aus $\mathfrak{G}$, die (x, y, z) auf $(x+a, y+b, z+c)$ abbildet, mit τ_{abc} , so ergibt sich

$$\begin{aligned} (x, y, z)^{\pi_i \tau_{abc} \pi_i^{-1}} &= (x+a, yw^i+b, zw^i+c)^{\pi_i^{-1}} \\ &= (x+a, y+bw^{-i}, z+cw^{-i}), \end{aligned}$$

d.h. es gilt

$$(2.15) \quad \pi_i \tau_{abc} \pi_i^{-1} = \tau_{a, bw^{-i}, cw^{-i}},$$

weswegen $\mathfrak{G}$ ein Normalteiler von $\mathfrak{U}$ ist. Da $\mathfrak{U}$ nach Definition von $\mathfrak{G}$ und $\mathfrak{H}$ erzeugt wird, ist es das semidirekte Produkt von $\mathfrak{G}$ mit $\mathfrak{H}$, siehe z.B. HALL 1959, Theorem 6.5.3. Aus (2.15) entnimmt man noch, daß es sich nicht um ein direktes Produkt handeln kann. Daher ist $\mathfrak{U}$ nicht abelsch.

Satz 2.3.6 besitzt folgende offensichtliche Verallgemeinerung:

2.3.7 Satz

Es sei $t=q_1 \dots q_n$ die Primzahlpotenzzzerlegung von t und r eine Primzahlpotenz mit $r \leq q_i$ für $i=1, \dots, n$. A sei die gemäß 2.3.1 und 2.3.2 über $EA(q_1^2) \oplus \dots \oplus EA(q_n^2)$ konstruierte K -Matrix und Π eine nach 2.2.6 und 2.2.9 über A konstruierte, bezüglich $\mathcal{Q} := \mathcal{J} \oplus EA(q_1^2) \oplus \dots \oplus EA(q_n^2)$ reguläre PK-Ebene. Dann läßt Π eine Kollineationsgruppe $\mathcal{K} \cong \mathbb{Z}_{q_1-1} \oplus \dots \oplus \mathbb{Z}_{q_n-1}$ zu, die auf Π' die Identität induziert. Die von $\mathcal{Q}$ und $\mathcal{K}$ erzeugte Kollineationsgruppe $\mathcal{U}$ von Π ist das semidirekte Produkt von $\mathcal{Q}$ mit $\mathcal{K}$. $\mathcal{U}$ ist nicht abelsch.

Beweis:

Wir setzen $\mathcal{K} := \{\pi_{i_1, \dots, i_n} : i_j = 0, \dots, q_j-2 \text{ für } j=1, \dots, n\}$ mit

$$(2.16) \quad \pi_{i_1, \dots, i_n} : (a, x_1, y_1, \dots, x_n, y_n) \mapsto$$

$$\mapsto (a, x_1 w_1^{i_1}, y_1 w_1^{i_1}, \dots, x_n w_n^{i_n}, y_n w_n^{i_n})$$

wobei $a \in \mathcal{J}$, $x_j, y_j \in EA(q_j)$ und w_j das für die Konstruktion von A verwendete erzeugende Element von $GF(q_j)^*$ ist ($j=1, \dots, n$).

Der Beweis verläuft nun genau wie der von Satz 2.3.6, wenn man (2.16) anstelle von (2.14) berücksichtigt.

2.4 Direkte Konstruktion von H-Matrizen

2.4.1 Lemma

Jede (r, r) -PK-Ebene Π ist sogar eine uniforme (r, r) -PH-Ebene.

Beweis:

Wir bezeichnen mit $\alpha(p)$ die durchschnittliche Anzahl von Verbindungsgeraden des Punktes p mit einem Nachbarpunkt $q \neq p$. Genau wie im Fall von PH-Ebenen (vgl. KLEINFELD 1950)

zeigt man, daß $\alpha(p)$ von der Wahl von p unabhängig ist, nämlich daß

$$(2.17) \quad \alpha(p) = \frac{t(r+1)}{t+1},$$

in unserem Falle also $\alpha(p) = r$ gilt. Da je zwei Punkte nach (PH 2) und Satz 2.1.2.(ii) höchstens r Verbindungsgeraden haben können, müssen also je zwei Nachbarpunkte genau r Verbindungsgeraden haben. Π erfüllt daher (PH 1) und aus Dualitätsgründen auch (PH 2). Daß (r, r) -PH-Ebenen uniform sind, ist wohlbekannt.

(Dieser Satz ist aus JUNGnickel 1975 übernommen).

2.4.2 Korollar

Für jede Primzahlpotenz q gibt es eine (q, q) -H-Matrix über $EA(q^2)$.

Beweis:

Nach 2.3.1 gibt es für jede Primzahlpotenz q eine (q, q) -K-Matrix über $EA(q^2)$, die nach 2.2.10 eine reguläre (q, q) -PK-Ebene definiert. Nach 2.4.1 handelt es sich daher sogar um eine reguläre (q, q) -PH-Ebene. Nochmalige Anwendung von 2.2.10 liefert die Behauptung.

2.4.3 Korollar

$(q, q) \in \mathfrak{R}$ für jede Primzahlpotenz q .

Im folgenden wiederholen wir um der Klarheit willen einige bekannte Definitionen und Resultate.

2.4.4 Definition

Ein Hjelmslev-Ring (kurz: H-Ring) ist ein assoziativer Ring mit $1 \neq 0$, für den gilt:

- (HR 1) Die Menge der Nicht-Einheiten (in Zukunft immer mit N bezeichnet) bildet ein zweiseitiges Ideal.
- (HR 2) N besteht aus zweiseitigen Nullteilern.

- (HR 3) Von je zwei Nullteilern ist einer ein rechtsseitiger Teiler des anderen.
- (HR 4) Von je zwei Nullteilern ist einer ein linksseitiger Teiler des anderen.

2.4.5 Satz

R sei ein H -Ring. Wir definieren die Inzidenzstruktur $\Pi(R)$ wie folgt:

Punkte sind die homogenen Tripel $\vec{E_p} = E(p_0, p_1, p_2)$, wo nicht alle p_i in N sind und $E := R \setminus N$ die Menge der Einheiten von R bezeichnet;

Geraden sind die homogenen Tripel $(u_0, u_1, u_2)^T E = \vec{u}^T E$, wo nicht alle u_i in N sind;

Inzidenz ist gegeben durch $\vec{E_p} \perp \vec{u}^T E$ genau dann, wenn $\vec{p} u^T = 0$.

Dann ist $\Pi(R)$ eine PH-Ebene. Falls $\text{card } N = t$ und $\text{card } R/N = r$ gilt, hat $\Pi(R)$ die Parameter t und r und $\Pi'(R)$ ist die desarguessche projektive Ebene der Ordnung r (wegen $R/N \cong GF(r)$).

Invertierbare 3×3 - Matrizen M über R erzeugen Kollineationen von $\Pi(R)$ gemäß

$$\vec{E_p} \mapsto E(\vec{p} M^{-1}) \quad \text{und} \quad \vec{u}^T E \mapsto (M u^T) E;$$

derartige Kollineationen werden wir als lineare Kollineationen von $\Pi(R)$ bezeichnen.

Beweis:

KLINGENBERG 1954. Ein ausführlicher Beweis findet sich in JUNGnickel 1975, Chapter 4.1.

2.4.6 Satz

Es sei $K := GF(q)$ und $R_n(q)$ der $n+1$ -dimensionale Vektorraum über K . $\{1, i, \dots, i^n\}$ sei eine Basis von $R_n(q)$. Wir setzen

$$\left(\sum_{j=0}^n a_j i^j \right) \left(\sum_{k=0}^n b_k i^k \right) := \sum_{j,k=0}^n a_j b_k i^{j+k}$$

mit $i^0 := 1$ und $i^1 := 0$ für $1 \geq n+1$. Dann ist $R_n(q)$ ein H -Ring mit Nullteilerideal $N := \langle i, \dots, i^n \rangle$. Die über $R_n(q)$ definierte PH-Ebene hat also die Parameter (q^n, q) .

Beweis:

Ein ausführlicher Beweis findet sich in JUNGnickel 1975 Chapter 4.1.

2.4.7 Satz

$R_n(q)$ und $\Pi := \Pi(R_n(q))$ seien wie in 2.4.6 und 2.4.5 erklärt. Dann gibt es $u, v, w \in GF(q)$, so daß

$$A := \begin{pmatrix} 0 & 0 & u \\ 1 & 0 & v \\ 0 & 1 & w \end{pmatrix}$$

eine zu $\mathbb{Z}_{q^2+q+1}$ isomorphe Gruppe von linearen Kollineationen von Π erzeugt, die auf Π' als Singergruppe (d.h. regulär) wirkt.

Auf $\mathfrak{N} := N \times N$ definiere man die Verknüpfung $*$ durch

$$(2.18) \quad (a, b) * (a', b') := \left(\frac{a+a'+(a'b+ab')v+bb'(u+vw)}{1+(a'b+ab')u+bb'uw}, \frac{b+b'+aa'+(a'b+ab')w+bb'(v+w^2)}{1+(a'b+ab')u+bb'uw} \right).$$

Durch (2.18) wird $(\mathfrak{N}, *)$ zu einer abelschen Gruppe (der Ordnung q^{2n}) und Π ist bezüglich $\mathbb{Z}_p \oplus \mathfrak{N}$ regulär (mit $p := q^2+q+1$).

Beweis:

Wir betrachten den Vektorraum $GF(q)^3$ über $GF(q)$ als Körper F , etwa mit erzeugendem Element α von F^* . Bekanntlich sind dann $1, \alpha, \alpha^2$ linear unabhängig über $GF(q)$, können also als Basis von $GF(q)^3$ gewählt werden. Ferner sei $\alpha^3 = u+v\alpha+w\alpha^2$. Die lineare Abbildung $x \mapsto \alpha x$ von $GF(q)^3$ in sich wird dann durch die in der Behauptung des Satzes angegebene Matrix A dargestellt. Der klassische Beweis des Satzes von SINGER 1938 (vgl. etwa auch LENZ 1965) zeigt dann, daß A eine zu $\mathbb{Z}_p$ ($p = q^2+q+1$) isomorphe Kollineationsgruppe der über $GF(q)$ konstruierten projektiven Ebene Π' erzeugt. Identifikation des Punktes (x, y, z) von Π' mit dem Punkt (x, y, z)

von Π (und der entsprechenden Geraden) liefert die Behauptung, da $GF(q)$ ein Unterkörper von $R_n(q)$ ist und A nach 2.4.5 auch eine Kollineation von Π induziert.

Wir betrachten jetzt lineare Nachbarkollineationen von Π , d.h. lineare Kollineationen, die jeden Punkt bzw. jede Gerade in einen Nachbarpunkt bzw. eine Nachbargerade abbilden. Sie werden genau von den Matrizen der Form

$$\begin{pmatrix} 1+c & d & g \\ a & 1+e & h \\ b & f & 1+k \end{pmatrix}$$

mit $a, b, c, d, e, f, g, h, k \in N$ erzeugt. Wir untersuchen, welche dieser Matrizen mit der Matrix A vertauschbar sind. Es ergibt sich

$$\begin{pmatrix} 0 & 0 & u \\ 1 & 0 & v \\ 0 & 1 & w \end{pmatrix} \begin{pmatrix} 1+c & d & g \\ a & 1+e & h \\ b & f & 1+k \end{pmatrix} = \begin{pmatrix} ub & uf & u+uk \\ 1+bv+c & d+vf & g+v+vk \\ a+bw & 1+e+wf & h+w+kw \end{pmatrix}$$

und

$$\begin{pmatrix} 1+c & d & g \\ a & 1+e & h \\ b & f & 1+k \end{pmatrix} \begin{pmatrix} 0 & 0 & u \\ 1 & 0 & v \\ 0 & 1 & w \end{pmatrix} = \begin{pmatrix} d & g & u+uc+vd+gw \\ 1+e & h & ua+v+ev+hw \\ f & 1+k & ub+vf+w+kw \end{pmatrix}.$$

Die resultierenden 9 Gleichungen ergeben, daß sich die Werte von a, b, c frei wählen lassen und die übrigen Größen d, e, f, g, h, k berechnet werden können. Da Division sämtlicher Matrixelemente durch den Nicht-Nullteiler $1+c$ die induzierte Kollineation nicht verändert, kann noch o.B.d.A. $c=0$ angenommen werden. Die resultierenden Gleichungen führen dazu, die Matrix $M(a, b)$ wie folgt zu definieren:

$$M(a, b) := \begin{pmatrix} 1 & bu & au+buw \\ a & 1+bv & av+b(u+vw) \\ b & a+bw & 1+aw+b(v+uw) \end{pmatrix}.$$

Die von $M(a, b)$ induzierte Kollineation sei mit $\sigma(a, b)$ bezeichnet. Wir untersuchen das Produkt $\sigma(a, b) \circ \sigma(a', b')$, das vom Produkt der Matrizen $M(a, b)$ und $M(a', b')$ erzeugt wird. Da beide Matrizen mit A vertauschbar sind, muß dasselbe auch für ihr Produkt gelten; nach eventuell notwendiger Normalisierung auf $c=0$ muß sich also ein $M(a'', b'')$

ergeben. Berechnung liefert $(a'', b'') = (a, b) * (a', b')$.

Wir weisen jetzt nach, daß $(\mathfrak{X}, *)$ eine abelsche Gruppe ist. $*$ ist offenbar kommutativ (die Definition ist symmetrisch in gestrichenen und ungestrichenen Größen) und läßt $(0, 0)$ als neutrales Element zu (dem entspricht die identische Kollineation $\sigma(0, 0)$). Wegen $\sigma(a, b) \circ \sigma(a', b') = \sigma((a, b) * (a', b'))$ ist $*$ auch assoziativ, da die Komposition von Abbildungen assoziativ ist. Schließlich ist die inverse Kollineation $\sigma^{-1}(a, b)$ wieder von der Form $\sigma(a', b')$, da mit $M(a, b)$ auch $M^{-1}(a, b)$ mit A vertauschbar ist; dann folgt $(a, b) * (a', b') = (0, 0)$.

Es sei $\mathfrak{S} := \{\sigma(a, b) : a, b \in N\}$. Nach dem Bisherigen gilt dann $(\mathfrak{S}, \circ) \cong (\mathfrak{X}, *)$, denn es ist $\sigma(a, b) \neq \sigma(a', b')$ für $(a, b) \neq (a', b')$: $M(a, b)$ führt nämlich $(1, 0, 0)^T$ in $(1, a, b)^T$ über und die Tripel $(1, a, b)^T$ und $(1, a', b')^T$ stellen verschiedene Geraden dar. Das zeigt zugleich, daß $\mathfrak{X}$ regulär auf der Nachbarklasse der Geraden $(1, 0, 0)^T$ operiert.

Sei nun $\mathfrak{L}$ die von A induzierte Kollineation von Π und $\mathfrak{U}$ die von $\mathfrak{L}$ erzeugte zyklische Gruppe der Ordnung p . $\mathfrak{M}$ sei die von $\mathfrak{U}$ und $\mathfrak{S}$ erzeugte abelsche Kollineationsgruppe von Π . Offenbar ist $\mathfrak{U} \cap \mathfrak{S} = 1$, also $\mathfrak{M} = \mathfrak{U} \oplus \mathfrak{S}$. Da $\mathfrak{U}$ auf der Menge der Geraden-Nachbarschaftsklassen von Π regulär ist und $\mathfrak{S}$ auf der Klasse von $(1, 0, 0)^T$ regulär ist, ist $\mathfrak{M}$ auf jeder Geradenklasse regulär und $\mathfrak{M}$ auf der Menge aller Geraden von Π regulär.

Wir betrachten nun den Punkt $(1, 0, 0)$, der durch $\sigma(a, b)^{-1}$ in den Punkt $(1, bu, au+buw)$ transformiert wird. Wir bemerken zunächst, daß $u \neq 0$ gelten muß; sonst hätten wir nämlich $\alpha^3 = v_0 + w_0^{-2}$ und $1, \alpha, \alpha^2$ wären doch linear abhängig. Daher sind die Gleichungen

$$bu = m \quad \text{und} \quad au+buw = n$$

für beliebige $m, n \in N$ (eindeutig) lösbar. Die Menge aller Punkte $(1, m, n)$ ist aber gerade die Nachbarklasse von $(1, 0, 0)$. Daher ist $\mathfrak{M}$ auf dieser und somit - wie oben - auf jeder Punktklasse regulär.

$\mathfrak{G}$ ist also auf jeder Punkt- und Geradenklasse und $\mathfrak{H}$ auf allen Punkten bzw. Geraden von Π regulär. Somit ist Π bezüglich $\mathbb{Z}_p \oplus \Pi$ regulär.

Wir bemerken, daß sich im Fall $n=1$ die nach (2.18) definierte Verknüpfung $*$ auf $N \times N$ auf die komponentenweise Addition reduziert; dann erhält man also $(\Pi, *) \cong \text{EA}(q^2)$.

2.4.8 Korollar

q sei Primzahlpotenz und n eine natürliche Zahl. Dann gibt es eine (q^n, q) -H-Matrix.

Beweis:

Das folgt aus 2.4.7 und 2.2.6.

2.4.9 Korollar

$(q^n, q) \in \mathfrak{H}$ für jede Primzahlpotenz q und jedes $n \in \mathbb{N}$.

2.5 Kompositionsmethoden zur Konstruktion von H-Matrizen

Bevor wir die allgemeinen Sätze entwickeln, geben wir zunächst ein Beispiel einer durch Komposition erhaltenen H-Matrix an.

2.5.1 Beispiel

Aus der (2,2)-H-Matrix über $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ (wie in Beispiel 2.2.12) und der folgenden (5,5)-H-Matrix über $\mathbb{Z}_5 \oplus \mathbb{Z}_5$ (nach 2.3.1 konstruiert)

$$\begin{pmatrix} (2,2) & (4,4) & (3,3) & (1,1) & (0,0) \\ (2,4) & (4,3) & (3,1) & (1,2) & (0,0) \\ (2,3) & (4,1) & (3,2) & (1,4) & (0,0) \\ (2,1) & (4,2) & (3,4) & (1,3) & (0,0) \\ (2,0) & (4,0) & (3,0) & (1,0) & (0,0) \\ (0,2) & (0,4) & (0,3) & (0,1) & (0,0) \end{pmatrix}$$

erhält man die folgende (10,2)-H-Matrix über

$\mathfrak{N} := \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$ (zur Vereinfachung der Darstellung schreiben wir für das Element (x,y,z,w) von $\mathfrak{N}$ kurz $xyzw$; die ersten beiden Ziffern sind also stets modulo 2, die letzten beiden modulo 5 zu rechnen):

$$\begin{pmatrix} 1122 & 1144 & 1133 & 1111 & 1100 & 0024 & 0043 & 0031 & 0012 & 0000 \\ 1023 & 1041 & 1032 & 1014 & 1000 & 0021 & 0042 & 0034 & 0013 & 0000 \\ 0120 & 0140 & 0130 & 0110 & 0100 & 0002 & 0004 & 0003 & 0001 & 0000 \end{pmatrix}$$

Man verifiziert direkt, daß es sich um eine H-Matrix handelt. Wir haben hier einen Spezialfall der folgenden allgemeinen Konstruktion vorzuliegen:

2.5.2 Satz

Wenn es eine (t,r) -H-Matrix und eine (s,q) -H-Matrix mit $q = t(r+1)-1$ gibt, so gibt es auch eine (st,r) -H-Matrix.

Beweis:

$A = (a_{ik})$ ($i=0,\dots,r$; $k=1,\dots,t$) sei eine (t,r) -H-Matrix und $B = (b_{ik})$ ($i=0,\dots,q$; $k=1,\dots,s$) sei eine (s,q) -H-Matrix. Wir definieren die $r+1 \times st$ -Matrix $C = (c_{ik})$ ($i=0,\dots,r$; $k=1,\dots,st$) wie folgt:

$$c_{ik} := (a_{i,\alpha k}; b_{it+\alpha k-1, k-(\alpha k-1)s}),$$

wobei αk die kleinste ganze Zahl $\geq \frac{k}{s}$ bezeichnet. Wir erhalten also

$$C = \begin{pmatrix} (a_{01}, b_{01}) \dots (a_{01}, b_{0s}) \dots (a_{0t}, b_{t-1,1}) \dots (a_{0t}, b_{t-1,s}) \\ (a_{11}, b_{t1}) \dots (a_{11}, b_{ts}) \dots (a_{1t}, b_{2t-1,1}) \dots (a_{1t}, b_{2t-1,s}) \\ \vdots \\ (a_{r1}, b_{rt,1}) \dots (a_{r1}, b_{rt,s}) \dots (a_{rt}, b_{q1}) \dots (a_{rt}, b_{qs}) \end{pmatrix}$$

C ist eine K-Matrix: Wir betrachten die Zeilen i und j ($i \neq j$, $i, j = 0, \dots, r$) und eine gegebene Differenz (x,y) . Da A eine K-Matrix ist, gibt es genau eine Darstellung $x = a_{ik} - a_{jl}$. Als Differenzen mit erster Koordinate x ergeben sich also alle Paare

$$(a_{ik}, b_{it+k-1, m}) - (a_{jl}, b_{jt+l-1, n})$$

mit $m, n = 1, \dots, s$. Wegen $i \neq j$ ist aber $it+k-1 \neq jt+l-1$; da B eine K-Matrix ist, durchlaufen also die zweiten Koordinaten der oben angegebenen Differenzen alle möglichen Werte, d.h. die Differenz (x, y) tritt wirklich auf. Also erfüllt C (2.9), ist also eine K-Matrix.

Wir zeigen nun, daß C sogar eine H-Matrix ist. Wir betrachten zunächst Differenzen mit erster Koordinate 0, etwa $(0, x)$ mit $x \neq 0$. Da B eine H-Matrix ist, tritt x mindestens zweimal in der Form $b_{jm} - b_{jn}$ auf. Nun gibt es aber Zahlen i und u ($i \in \{0, \dots, r\}$, $u \in \{0, \dots, t-1\}$) mit

$$j = it + \alpha(us+1) - 1;$$

$$\text{dann gilt } (0, x) = (a_{i, \alpha(us+m)}, b_{jm}) - (a_{i, \alpha(us+n)}, b_{jn})$$

$= c_{i, us+m} - c_{i, us+n}$; also tritt die Differenz $(0, x)$ in C zweimal auf.

Sei nun eine Differenz (x, y) mit $x \neq 0$ gegeben. Da A eine H-Matrix ist, tritt x mindestens zweimal in der Form $x = a_{ik} - a_{il}$ auf. Dann haben alle Differenzen

$$(a_{ik}, b_{it+k-1, m}) - (a_{il}, b_{it+l-1, n})$$

für $m, n = 1, \dots, s$ als erste Koordinate x. Wegen $k \neq l$ durchlaufen dann die zweiten Koordinaten alle möglichen Werte, da B eine K-Matrix ist. Daher tritt die Differenz (x, y) in C mindestens zweimal auf; C ist also eine H-Matrix.

Für $t=r=2$ und $q=s=5$ liefert der Satz unser Beispiel 2.5.1.

2.5.3 Korollar

q und r seien Primzahlpotenzen mit $q = t(r+1)-1$. Gilt dann $(t, r) \in \mathcal{R}_1$ und $(s, q) \in \mathcal{R}_2$, so gilt auch $(st, r) \in \mathcal{R}_2$. Insbesondere folgt aus $(t, r) \in \mathcal{R}_2$ stets $(tq^n, r) \in \mathcal{R}_2$.

Beweis:

Das folgt aus 2.5.2, 2.2.10 und 2.4.9.

Korollar 2.5.3 entspricht 2.1.5.(i) mit $\mathcal{R}_2$ statt $\mathcal{S}_2$.

2.5.4 Beispiele

r	2						
t	2	4	8	10	16	44	50
q	5	11	23	29	47	131	149
s	5^n	11^n	23^n	29^n	47^n	131^n	149^n
st	$2 \cdot 5^n$	$4 \cdot 11^n$	$8 \cdot 23^n$	$10 \cdot 29^n$	$16 \cdot 47^n$	$44 \cdot 131^n$	$50 \cdot 149^n \dots$

Man beachte, daß für $t = 10, 44, 50$ die Konstruktion zweimal benutzt wurde. Man erhält so zu den bereits bekannten Parameterpaaren $(2^n, 2) \in \mathfrak{R}_2$ ($n=0, \dots, 9$) 8 weitere Paare $(x, 2) \in \mathfrak{R}_2$ mit $x \leq 1000$.

r	3			4		5	
t	3	27	33	4	16	5	25
q	11	107	131	19	79	29	149
s	11^n	107^n	131^n	19^n	79^n	29^n	149^n
st	$3 \cdot 11^n$	$27 \cdot 107^n$	$33 \cdot 131^n$	$\dots 4 \cdot 19^n$	$16 \cdot 79^n$	$\dots 5 \cdot 29^n$	$25 \cdot 149^n \dots$

Zu den bekannten 7 Paaren $(3^n, 3)$ ($n=0, \dots, 6$) kommen zwei weitere Paare $(x, 3) \in \mathfrak{R}_3$ mit $x \leq 1000$.

Nochmalige Anwendung der Konstruktion liefert wieder $(2 \cdot 5 \cdot 29^n, 2) \in \mathfrak{R}_2$, was aber schon bekannt ist. Wir kennen nun 18 Paare $(x, 2)$ und 9 Paare $(x, 3) \in \mathfrak{R}_2$ mit $x \leq 1000$.

Um Satz 2.5.2 weiter verallgemeinern zu können, benötigen wir den folgenden zentralen Begriff:

2.5.5 Definition

$A = (a_{ik})$ sei eine (t, r) -H-Matrix. Eine x-Auswahl für A besteht aus je x Elementen aus jeder Zeile von A, so daß gilt:

(2.19) Unter allen Differenzen der Formen

$$x_i - a_{ik} \quad \text{und} \quad a_{ik} - x_i$$

- wobei x_i ein aus der i-ten Zeile ausgewähltes Element bezeichnet und a_{ik} alle Elemente $\neq x_i$ aus der i-ten Zeile durchläuft - kommt jedes Element $\neq 0$ insgesamt mindestens zweimal vor.

2.5.6 Satz

Wenn es eine (t,r) -H-Matrix mit einer z -Auswahl und eine (s,q) -H-Matrix mit

$$(2.20) \quad (z+1)(r+1) \leq q+1 \leq t(r+1)$$

gibt, so gibt es auch eine (st,r) -H-Matrix mit einer $s.pq$ -Auswahl, wo pq die kleinste ganze Zahl $> \frac{q+1}{r+1}$ bezeichnet.

Beweis:

Es sei $A = (a_{ik})$ ($i=0, \dots, r$; $k=1, \dots, t$) eine (t,r) -H-Matrix mit einer z -Auswahl $\mathfrak{z}$. Wegen 2.2.11.(i) können wir o.B.d.A. annehmen, daß $\mathfrak{z}$ aus den Elementen a_{ik} mit $i=0, \dots, r$ und $k=1, \dots, z$ besteht.

Ferner sei $B = (b_{ik})$ ($i=0, \dots, s$; $k=1, \dots, q$) eine (s,q) -H-Matrix und $M = \{0, \dots, q\}$. Wir zerlegen M in disjunkte Teilmengen $M_0, \dots, M_r$ mit

$$(2.21) \quad z+1 \leq \text{card } M_i \leq pq \leq t \text{ für } i=0, \dots, r,$$

was wegen (2.20) möglich ist. Wir wählen nun für jedes $i \in \{0, \dots, r\}$ eine surjektive Abbildung $\pi_i: \{1, \dots, t\} \rightarrow M_i$, so daß gilt

$$(2.22) \quad \pi_i(k) \neq \pi_i(1) \quad \text{für } k \neq 1 \text{ mit } k=1, \dots, z \\ \text{und } 1 = 1, \dots, t$$

und

$$(2.23) \quad \pi_i(\{1, \dots, pq\}) = M_i,$$

was wegen (2.21) möglich ist.

Wir definieren eine $r+1 \times st$ -Matrix $C = (c_{ik})$ mit $i=0, \dots, r$ und $k=1, \dots, st$ durch

$$c_{ik} := (a_{i, \alpha k}; b_{\pi_i(\alpha k), k - (\alpha k - 1)s}),$$

wobei αk die kleinste ganze Zahl $\geq \frac{k}{s}$ bezeichnet. Wir erhalten also

$$C = \begin{pmatrix} (a_{01}, b_{\pi_0(1), 1}) \dots (a_{01}, b_{\pi_0(1), s}) \dots (a_{0t}, b_{\pi_0(t), 1}) \dots (a_{0t}, b_{\pi_0(t), s}) \\ \vdots \\ (a_{r1}, b_{\pi_r(1), 1}) \dots (a_{r1}, b_{\pi_r(1), s}) \dots (a_{rt}, b_{\pi_r(t), 1}) \dots (a_{rt}, b_{\pi_r(t), s}) \end{pmatrix}$$

C ist eine K-Matrix: Wir betrachten die Zeilen i und j mit $i \neq j$ und $i, j \in \{0, \dots, r\}$. Ist eine Differenz (x, y) gegeben, so gibt es, da A eine K-Matrix ist, genau eine Darstellung $x = a_{ik} - a_{il}$. Als Differenzen mit erster Koordinate x ergeben sich also genau die Paare

$$(a_{ik}, b_{\pi_{ik}, m}) - (a_{jl}, b_{\pi_{jl}, n})$$

mit $m, n = 1, \dots, s$. Nach Konstruktion gilt aber $\pi_{ik} \neq \pi_{jl}$; da B eine K-Matrix ist, durchlaufen die angegebenen Differenzen also alle Paare (x, y) . Somit ist auch C eine K-Matrix.

Wir zeigen nun, daß C sogar eine H-Matrix ist. Zunächst betrachten wir Differenzen mit erster Koordinate 0, etwa $(0, x)$ mit $x \neq 0$. Da B H-Matrix ist, tritt x mindestens zweimal in der Form $x = b_{im} - b_{in}$ auf. Da die π_l surjektiv sind, gibt es Indizes h, j mit $\pi_h j = i$, d.h. in der h-ten Zeile von C tritt die Differenz $(a_{hj}, b_{\pi_{hj}, m}) - (a_{hj}, b_{\pi_{hj}, n}) = (0, x)$ auf. Daher tritt auch in C jede Differenz $(0, x)$ mindestens zweimal auf.

Sei nun ein beliebiges Paar (x, y) mit $x \neq 0$ gegeben. Da $\mathfrak{A}$ eine z-Auswahl von A ist, tritt x mindestens zweimal als Differenz der Form

$$x = a_{ik} - a_{il} \quad \text{bzw.} \quad x = a_{il} - a_{ik}$$

mit $k \in \{1, \dots, z\}$ auf. Wir betrachten o.B.d.A. den Fall $x = a_{ik} - a_{il}$. Nach (2.22) gilt $\pi_{ik} \neq \pi_{il}$; da B eine K-Matrix ist, gibt es also eindeutig bestimmte Indizes m, n mit

$$y = b_{\pi_{ik}, m} - b_{\pi_{il}, n},$$

woraus sich ergibt

$$(x, y) = (a_{ik}, b_{\pi_{ik}, m}) - (a_{il}, b_{\pi_{il}, n}).$$

Verfährt man analog für die zweite Darstellung von x, ergibt sich die Gültigkeit von (2.10) für C. C ist also eine H-Matrix.

Es bleibt zu zeigen, daß C eine s, p, q-Auswahl besitzt. Wir behaupten, daß die Elemente c_{ik} mit $i=0, \dots, r$ und $k=1, \dots, pq$

eine derartige Auswahl bilden. Die vorstehende Argumentation zeigt, daß Differenzen der Form (x,y) mit $x \neq 0$ mindestens zweimal als

$$(x,y) = c_{ik} - c_{il} \quad \text{bzw.} \quad (x,y) = c_{il} - c_{ik}$$

mit $k \in \{1, \dots, sz\}$ auftreten; daher ist für diese Differenzen die Behauptung wegen $z+1 \leq pq$ gültig.

Schließlich zeigt der oben durchgeführte Beweis der Tatsache, daß die Differenzen mit erster Koordinate 0 in C mindestens zweimal auftreten, auch den Rest der Behauptung; mit den dort angegebenen Bezeichnungen kann man nämlich wegen (2.23) den Index j aus der Menge $\{1, \dots, pq\}$ wählen. Damit ist der Beweis des Satzes vollständig.

Wir bemerken, daß sich Satz 2.5.2 als triviales Korollar aus Satz 2.5.6 ergibt, da jede (t,r) -H-Matrix offenbar eine $(t-1)$ -Auswahl zuläßt. Wir haben den Beweis von 2.5.2 trotzdem durchgeführt, weil uns das den allgemeinen Fall besser zu motivieren scheint.

2.5.7 Lemma

Jede (r,r) -H-Matrix besitzt eine 1-Auswahl.

Beweis:

Wir wählen etwa die Elemente a_{i1} für $i=0, \dots, r$ aus. Die Differenzen $a_{i1} - a_{i2}, \dots, a_{i1} - a_{ir}$ sind nach 2.2.11 für festes i alle verschieden; nach (2.9) kann aber auch nicht gelten $a_{i1} - a_{ik} = a_{j1} - a_{j1}$ für $i \neq j$; denn dann folgte $a_{i1} - a_{j1} = a_{ik} - a_{j1}$, im Widerspruch zu (2.9). Wir erhalten also so bereits $(r+1)(r-1) = r^2 - 1$ verschiedene Differenzen je einmal, d.h. alle möglichen Differenzen je einmal. Analog zeigt man, daß auch alle möglichen Differenzen je einmal in der Form $a_{ik} - a_{i1}$ ($k \neq 1$, $i=0, \dots, r$, $k=2, \dots, r$) auftreten. Also ist (2.19) erfüllt.

2.5.8 Korollar

q und r seien Primzahlpotenzen mit $2(r+1) \leq q+1 \leq r(r+1)$.

Falls es eine (s, q) -H-Matrix gibt, gibt es auch eine (rs, r) -H-Matrix mit einer $s \cdot pq$ -Auswahl; dabei bezeichnet pq die kleinste ganze Zahl $\geq \frac{q+1}{r+1}$.

Beweis:

Das folgt unmittelbar aus 2.4.2, 2.5.7 und 2.5.6.

2.5.9 Korollar

q und r seien Primzahlpotenzen mit $2(r+1) \leq q+1 \leq r(r+1)$. Falls gilt $(s, q) \in \mathcal{H}$, gilt auch $(sr, r) \in \mathcal{H}$. Insbesondere ist stets $(q^n r, r) \in \mathcal{H}$.

Beweis:

Das folgt unmittelbar aus 2.5.8, 2.4.9 und 2.2.10.

2.5.10 Beispiele

Wir geben nur solche Parameterserien an, die nicht schon nach 2.4.9 bzw. 2.5.4 bekannt sind.

r	3		4				5			
q	7	8	9	11	13	17	11	13	16	
s	7^n	8^n	9^n	11^n	13^n	17^n	11^n	13^n	16^n	
sr	$3 \cdot 7^n$	$3 \cdot 8^n$	$4 \cdot 9^n$	$4 \cdot 11^n$	$4 \cdot 13^n$	$4 \cdot 17^n$	$5 \cdot 11^n$	$5 \cdot 13^n$	$5 \cdot 16^n$	

r	5				7				
q	17	19^n	23	27	16	17	19	23	
s	17^n	19^n	23^n	27^n	16^n	17^n	19^n	23^n	
sr	$5 \cdot 17^n$	$5 \cdot 19^n$	$5 \cdot 23^n$	$5 \cdot 27^n$	$7 \cdot 16^n$	$7 \cdot 17^n$	$7 \cdot 19^n$	$7 \cdot 23^n$	etc.

Nochmalige Anwendung von 2.5.9 liefert u.a.

r	2								
q	5								
s	$5 \cdot 11^n$	$5 \cdot 13^n$	$5 \cdot 16^n$	$5 \cdot 17^n$	$5 \cdot 19^n$	$5 \cdot 23^n$	$5 \cdot 27^n$		
sr	$10 \cdot 11^n$	$10 \cdot 13^n$	$10 \cdot 16^n$	$10 \cdot 17^n$	$10 \cdot 19^n$	$10 \cdot 23^n$	$10 \cdot 27^n$		

Zu den 18 nach 2.4.9 und 2.5.4 bekannten Paaren $(x, 2) \in \mathcal{H}$ mit $x \leq 1000$ kommen also 7 weitere hinzu. Entsprechend erhält man zu den 9 bisher bekannten Paaren $(x, 3) \in \mathcal{H}$ mit $x \leq 1000$ 39 weitere, nämlich

$$x = 3 \cdot 7, 3 \cdot 49, 3 \cdot 8, 3 \cdot 64;$$

$$x = 3 \cdot 7 \cdot q, \quad q \text{ Primzahlpotenz mit } 16 \leq q \leq 47;$$

$$x = 3 \cdot 8 \cdot q, \quad q \text{ Primzahlpotenz mit } 17 \leq q \leq 41;$$

$$x = 3 \cdot 9 \cdot q, \quad q \text{ Primzahlpotenz mit } 19 \leq q \leq 37;$$

$$x = 3 \cdot 11 \cdot q, \quad q \text{ Primzahlpotenz mit } 23 \leq q \leq 29.$$

Korollar 2.5.9 entspricht Satz 2.1.5.(ii), aber wieder mit $\mathfrak{A}$ anstelle von $\mathfrak{B}$.

2.5.11 Satz

q und r seien Primzahlpotenzen mit $2(r+1) \leq q+1 \leq r(r+1)$ und es gebe eine (s, q) -H-Matrix. q' sei eine weitere Primzahlpotenz mit $(s \cdot \rho q + 1)(r+1) \leq q'+1 \leq sr(r+1)$ und es gebe eine (s', q') -H-Matrix. Dabei sei ρq wieder die kleinste ganze Zahl $\geq \frac{q+1}{r+1}$. Dann gibt es auch eine $(ss'r, r)$ -H-Matrix mit einer $s' \cdot \rho q'$ -Auswahl.

Beweis:

Das folgt unmittelbar aus 2.5.6 und 2.5.8.

2.5.12 Korollar

q und r seien Primzahlpotenzen mit $2(r+1) \leq q+1 \leq r(r+1)$. Es gelte $(s, q) \in \mathfrak{A}$ und $(s', q') \in \mathfrak{A}$, wo q' eine weitere Primzahlpotenz ist mit $(s \cdot \rho q + 1)(r+1) \leq q'+1 \leq sr(r+1)$ und ρq wie üblich die kleinste ganze Zahl $\geq \frac{q+1}{r+1}$ bezeichnet. Dann ist auch $(ss'r, r) \in \mathfrak{A}$, insbesondere stets $(sq'^n r, r) \in \mathfrak{A}$.

Beweis:

Das folgt unmittelbar aus 2.5.11, 2.4.9 und 2.2.10.

2.5.13 Beispiele

Für $r=3$ und $q=s=7$ erhält man $(3 \cdot 7 \cdot q'^n, 3) \in \mathfrak{A}$ für Primzahlpotenzen q' mit $59 \leq q' \leq 83$; durch zweimalige Anwendung von 2.5.9 erhält man das entsprechende Resultat für $16 \leq q' \leq 55$. 2.5.12 liefert also Paare in $\mathfrak{A}$, die wir noch nicht kannten. Wir bemerken, daß man für diese Paare bisher nicht einmal wußte, ob sie in $\mathfrak{A}$ liegen; sie sind

mit Satz 2.1.5 offenbar nicht zu erhalten. Unsere Konstruktion ergibt also auch bisher unbekannte Parameterpaare für PH-Ebenen. Allgemein erhält man durch zweimalige Anwendung von 2.5.9 im Falle $s=q$ (q'^n_{qr}, r) $\in \mathfrak{H}_5$ für

$$(2.24) \quad q' \text{ Primzahlpotenz mit } 2(q+1) \leq q'+1 \leq q(q+1),$$

nach 2.5.12 hingegen für

$$(2.25) \quad q' \text{ Primzahlpotenz mit } (q_{\rho}q+1)(r+1) \leq q'+1 \leq qr(r+1).$$

Die obere Grenze in (2.25) ist besser als die in (2.24), sofern nur $q < r(r+1)-1$ gilt (was das nach 2.5.9 maximal mögliche q ist). Damit (2.25) anwendbar ist, muß allerdings noch $\rho q < r$ werden, d.h. wir müssen noch $q+1 \leq (r-1)(r+1) = r^2-1$ fordern.

Für $r=3$, $s=q=8, 9, 11$ ist (2.25) also nicht anwendbar; aber z.B. für $r=5$, $s=q=11, 13, 16, 17, 19, 23$. Man sieht, daß wir für jede Primzahlpotenz ≥ 3 bisher unbekannte Parameterserien erhalten.

Wir bemerken, daß die nach (2.24) konstruierten Matrizen nach 2.5.6 eine $q'^n_{\rho q}$ -Auswahl besitzen, die nach (2.25) konstruierten jedoch wegen 2.5.11 eine $q'^n_{\rho q'}$ -Auswahl. In beiden Fällen läßt sich das Konstruktionsverfahren durch weitere Anwendung von 2.5.6 fortsetzen; man benötigt eine weitere Primzahlpotenz q'' , die im ersten Fall

$$(2.26) \quad (q'^n_{\rho q}q+1)(r+1) \leq q''+1 \leq q'^n_{qr}(r+1)$$

bzw. im zweiten Fall

$$(2.27) \quad (q'^n_{\rho q'}+1)(r+1) \leq q''+1 \leq q'^n_{qr}(r+1)$$

erfüllt, und erhält dann $(q'^k_{q'}q'^n_{qr}, r)$ -H-Matrizen mit entsprechender Auswahl. In beiden Fällen erhält man bisher unbekannte Parameterpaare; im ersten Fall erhält man z.B. für $r=3$, $q=s=7$, $q'=16$, $n=1$ die Paare $(3 \cdot 7 \cdot 16 \cdot q''^v, 3)$ für Primzahlpotenzen q'' mit $899 \leq q'' \leq 1349$, durch nochmalige Anwendung von 2.5.9 hingegen für $33 < q'' < 271$.

Im zweiten Fall erhält man z.B. für $r=3$, $q=s=7$, $q'=50$, $n=1$ Parameterpaare $(3 \cdot 7 \cdot 50 \cdot q''^k, 3)$ für Primzahlpotenzen q'' mit $3539 \leq q'' \leq 4956$, durch Anwendung von 2.5.9 hingegen für $119 \leq q'' \leq 3539$.

Es ist klar, daß das Verfahren fortgesetzt werden kann, um weitere neue Parameterserien zu liefern.

Bisher haben wir Satz 2.5.6 auf (r,r) -Matrizen mit Auswahlen angewandt. Es liegt nahe, auch nach Auswahlen von (q^n, q) -H-Matrizen - wie in 2.4.7 konstruiert - zu suchen. Um ein zu 2.5.7 analoges Lemma zu beweisen, benötigen wir zunächst einige Hilfsaussagen über den H-Ring $R_n(q)$.

2.5.14 Lemma

$R_n(q)$ sei der in 2.4.6 eingeführte H-Ring und N wie dort definiert. Ferner sei $N' := \langle i, \dots, i^{n-1} \rangle$, $N'' := \langle i^n \rangle$ und $H := \langle 1, i^n \rangle$.

Für jedes $m \in N$ bezeichne m' den Anteil von m aus N' und m'' den Anteil von m aus N'' ; genauer gesagt:

(2.28) Ist $m = m_1 i + m_2 i^2 + \dots + m_n i^n$, so setzen wir

$$m' := m_1 i + m_2 i^2 + \dots + m_{n-1} i^{n-1} \quad \text{und}$$

$$m'' := m_n i^n.$$

Ferner sei $R_2(q) = \langle 1, j \rangle$ H-Ring wie in 2.4.6 beschrieben. Dann gilt:

- (i) H ist ein zu $R_2(q)$ isomorpher Unterring von $R_n(q)$.
- (ii) $(N \times N, *) \cong (N' \times N', *) \oplus (N'' \times N'', *)$
(Hier sei $*$ wie in 2.4.7 erklärt, die Einschränkung auf $N' \times N'$ bzw. $N'' \times N''$ wieder mit $*$ bezeichnet und $\oplus$ bedeute die Bildung des direkten Produktes.)
- (iii) $(N'' \times N'', *) \cong EA(q) \oplus EA(q) \cong (M \times M, *)$

(Dabei sei $M := \langle j \rangle$ und $*$ wieder die nach 2.4.7 auf $M \times M$ erklärte Verknüpfung).

(iv) Es seien $m, k \in \mathbb{N}$. Dann gilt für jedes $x \in GF(q)$

$$\frac{m}{k+x} = \frac{m'}{k'+x} + \frac{m''}{k''+x} \quad (x \neq 0)$$

Beweis:

(i) Offenbar ist H eine additive Untergruppe von $R_n(q)$.
 H ist multiplikativ abgeschlossen, denn

$$(a+bi^n)(c+di^n) = ab+(ac+bd)i^n \quad \text{f.a. } a, b, c, d \in GF(q) \text{ und}$$

$$(a+bi^n)\left(\frac{1}{a} - \frac{b}{a^2} i^n\right) = 1 \quad \text{f.a. } a, b \in GF(q) \text{ mit } a \neq 0.$$

Wegen $(a+bj)(c+dj) = ab+(ac+bd)j$ ist die Abbildung

$$a+bi^n \mapsto a+bj$$

ein Isomorphismus zwischen H und $R_2(q)$.

(ii) Es gilt $(a, b) = (a', b') * (a'', b'')$ für alle $a, b \in \mathbb{N}$ nach (2.18), weil die dort auftretenden gemischten Terme $a'a''$, $a'b''$, $b'b''$ und $a''b'$ sämtlich verschwinden, da sie nur höhere Potenzen von i als die n -te Potenz enthalten.

Unmittelbar nach Definition gilt $N' \times N' \subset N'' \times N'' = \{(0, 0)\}$.

Da $N \times N$ abelsch ist, also jede Untergruppe ein Normalteiler, folgt somit die Behauptung (siehe z.B. HALL 1960, Theorem 2.5.1).

(iii) Es gilt $(ai^n, bi^n) * (ci^n, di^n) = (ai^n+ci^n, bi^n+di^n)$, da die gemischten Glieder sämtlich die Potenz $i^{2n} = 0$ enthalten. Die Isomorphie $(N'' \times N'', *) \cong EA(q) \oplus EA(q)$ ist also klar. Analog zeigt man $EA(q) \subset EA(q) \cong (M \times M, *)$.

(iv) Es sei etwa $k = k_1 i + \dots + k_n i^n$. Wir berechnen das Inverse von $x+k$ und setzen $k_0 := x$. Ist das Inverse $a_0 + a_1 i + \dots + a_n i^n$, ergibt sich

$$k_0 a_0 = 1$$

$$k_1 a_0 + a_1 k_0 = 0$$

....

$$(2.20) \quad k_n a_0 + k_{n-1} a_1 + \dots + k_0 a_n = 0$$

Der Koeffizient k_n geht erst in (2.29) ein, die Elemente $(k+x)^{-1}$ und $(k'+x)^{-1}$ unterscheiden sich also erst in der i^n -Komponente. Ist daher 1 ein beliebiger Nullteiler, so unterscheiden sich $1(k+x)^{-1}$ und $1(k'+x)^{-1}$ überhaupt nicht:

$$(2.30) \quad \frac{1}{k+x} = \frac{1}{k'+x} \quad \text{für alle } k, l \in N, x \in GF(q), x \neq 0.$$

Als nächstes betrachten wir $(k''+x)^{-1}$. Dieses Element ist $x^{-1} - k_n x^{-2} i^n$. Durch Multiplikation mit einem beliebigen Nullteiler 1 wird daraus $\frac{1}{x}$, also

$$(2.31) \quad \frac{1}{k''+x} = \frac{1}{x} \quad \text{für alle } k, l \in N, x \in GF(q), x \neq 0.$$

Schließlich untersuchen wir nochmals $(k+x)^{-1} = x^{-1} + a_1 i + \dots + a_n i^n$ (s.o.). Multiplikation mit $1'' \in N''$ ergibt $1'' x^{-1}$, also

$$(2.32) \quad \frac{1''}{k+x} = \frac{1''}{x} \quad \text{für alle } k, l \in N, x \in GF(q), x \neq 0.$$

Aus (2.30) bis (2.32) folgt dann für alle $k, m \in N$, $x \in GF(q)$ mit $x \neq 0$

$$\frac{m}{k+x} = \frac{m'}{k'+x} + \frac{m''}{k''+x} = \frac{m'}{k'+x} + \frac{m''}{x} = \frac{m'}{k'+x} + \frac{m''}{1''+x}.$$

2.5.15 Lemma

Für jede Primzahlpotenz q und jede natürliche Zahl n gibt es eine (q^n, q) -H-Matrix mit einer q^{n-1} -Auswahl.

Beweis:

Für $n=1$ gilt das bereits nach 2.4.2 und 2.5.7. Sei also jetzt $n \neq 1$. Wir betrachten die in 2.4.7 konstruierte reguläre (q^n, q) -PH-Ebene.

Im Beweis von Satz 2.2.6 haben wir folgendes gezeigt:

In einer bezüglich $0 = g \oplus n$ regulären PH-Ebene wähle man

einen Basispunkt, koordinatisiere dann alle Punkte durch $\mathfrak{g}$, wähle eine Basisgerade und fasse sie als Punktmenge auf. Diese Basisgerade ist dann eine spezielle Differenzenmenge.

Aus Dualitätsgründen gilt daher auch folgendes: Man wähle eine Basisgerade, koordinatisiere die Geraden durch $\mathfrak{g}$, wähle einen Basispunkt und fasse ihn als Geradenmenge auf. Dieser Basispunkt ist dann eine spezielle Differenzenmenge, aus der man nach 2.2.9 eine H-Matrix erhält.

Wir führen dieses Verfahren mit dem Basispunkt $(0,0,1)$ unserer gegebenen regulären PH-Ebene durch. Die zugehörige Geradenmenge besteht genau aus den Geraden

$$(1, x+m, 0)^T \text{ und } (m, 1, 0)^T \text{ mit } x \in GF(q) \text{ und } m \in N.$$

Wir müssen die Koordinaten dieser Geraden bezüglich $\mathfrak{g}$ bestimmen (als Basisgerade sei $(1,0,0)^T$ gewählt). Da wir nur an der entstehenden H-Matrix interessiert sind, ist die sich aus $\mathfrak{g}$ ergebende Koordinate uninteressant, da sie nur die Nachbarschaftsklasse angibt; wir benötigen nur die sich aus $\mathfrak{H} = N \times N$ ergebenden Koordinaten. Wir müssen also die Matrix $M(a,b)$ (wie auf S.29 unten definiert) bestimmen, die $(0,1,0)^T$ in $(m,1,0)^T$ bzw. $(1,x,0)^T$ in $(1,x+m,0)^T$ überführt.

Im ersten Fall erhalten wir

$M(a,b)(0,1,0)^T = (bu, 1+bv, a+bw)^T \stackrel{!}{=} (m, 1, 0)^T$, woraus sich die Bedingungen

$$(2.33) \quad bu = m(1+bv) \quad \text{und} \quad a+bw = 0$$

ergeben. (2.33) ist wegen $u \neq 0$ (vgl. S.30 unten) eindeutig lösbar; als Koordinaten von $(m,1,0)^T$ ergeben sich dann

$$(2.34) \quad a = \frac{-mw}{u-mv} \quad \text{und} \quad b = \frac{m}{u-mv}.$$

Im zweiten Fall erhalten wir

$M(a,b)(1,x,0)^T = (1+bux, a+x+bvx, b+ax+bwx)^T \stackrel{!}{=} (1, x+m, 0)^T$, woraus sich die Bedingungen

$$(2.35) \quad a+x+bvx = (x+m)(1+bux) \quad \text{und}$$

$$(2.36) \quad b+ax+bwx = 0$$

ergeben. (2.35) liefert

$$(2.37) \quad a = b(ux^2 + uxm - vx) + m,$$

Einsetzen in (2.36) ergibt

$$(2.38) \quad b(1 + wx + ux^3 + ux^2m - vx^2) = -mx.$$

Nun muß $1 + wx + ux^3 - vx^2 \neq 0$ sein; das ist für $x=0$ klar.

Für $x \neq 0$ wäre sonst $vx^2 = 1 + wx + ux^3$. Mit den Bezeichnungen des Beweises von 2.4.7 folgte dann

$$x^2 \alpha^3 = ux^2 + v \alpha x^2 + w \alpha^2 x^2 = ux^2 + c + \alpha wx + \alpha ux^3 + w \alpha^2 x^2,$$

also

$$(1 + \alpha x)(ux^2 + c + (wx + 1) - x \alpha^2) = 0,$$

im Widerspruch zur linearen Unabhängigkeit von $1, \alpha, \alpha^2$.

Daher sind (2.38) und (2.37) (eindeutig) lösbar und wir erhalten als Koordinaten von $(1, x + m, 0)^T$

$$(2.39) \quad a = \frac{m(1 + wx)}{1 + wx + ux^3 - vx^2 + ux^2m} \quad \text{und}$$

$$b = \frac{-mx}{1 + wx + ux^3 - vx^2 + ux^2m}.$$

Wir erhalten also eine (q^n, q) -H-Matrix mit Zeilen

$$\left\{ \left(\frac{-mw}{u - mv}, \frac{m}{u - mv} \right) : m \in N \right\} =: Z_q$$

und

$$\left\{ \left(\frac{m(1 + wx)}{1 + wx + ux^3 - vx^2 + ux^2m}, \frac{-mx}{1 + wx + ux^3 - vx^2 + ux^2m} \right) : m \in N \right\} =: Z_x$$

für jedes $x \in \text{GF}(q)$.

Nach Lemma 2.5.14 gilt aber

$$\left(\frac{-mw}{u - mv}, \frac{m}{u - mv} \right) = \left(\frac{-m'w}{u - m'v}, \frac{m'}{u - m'v} \right) * \left(\frac{-m''w}{u - m''v}, \frac{m''}{u - m''v} \right),$$

weswegen wir zerlegen können:

$$\begin{aligned} Z_q &= \left\{ \left(\frac{-m'w}{u - m'v}, \frac{m'}{u - m'v} \right) : m' \in N' \right\} \otimes \left\{ \left(\frac{-m''w}{u - m''v}, \frac{m''}{u - m''v} \right) : m'' \in N'' \right\} \\ &=: Z_q' \otimes Z_q''. \end{aligned}$$

Analog ergibt sich für jedes $x \in \text{GF}(q)$ eine Zerlegung

$$Z_x = Z_x' \otimes Z_x''.$$

Nach Lemma 2.5.14.(i) und dem Bisherigen enthält die betrachtete reguläre PH-Ebene $\Pi = \Pi(n, q)$ eine zu $\pi(\sigma, q)$ iso-

morphe Unterstruktur, zu der die (q, q) -H-Matrix mit den Zeilen Z_q'' und Z_x'' ($x \in \text{GF}(q)$) gehört.

Diese H-Matrix besitzt nach 2.5.7 eine 1-Auswahl (wir können z.B. aus jeder Zeile das Paar $(0, 0)$ auswählen, welches sich für $m'' = 0$ ergibt). Daher ist dann

$$Z_q' \otimes \{(0, 0)\}$$

zusammen mit

$$Z_x' \otimes \{(0, 0)\} \quad \text{für alle } x \in \text{GF}(q)$$

eine q^{n-1} -Auswahl der konstruierten (q^n, q) -H-Matrix.

2.5.16 Satz

Es seien r und q Primzahlpotenzen mit

$$(2.40) \quad (r^{n-1} + 1)(r + 1) \leq q + 1 \leq r^n(r + 1)$$

und es gebe eine (s, q) -H-Matrix. ρq bezeichne wieder die kleinste ganze Zahl $\geq \frac{q+1}{r+1}$. Dann gibt es auch eine

(sr^n, r) -H-Matrix mit einer $s \cdot \rho q$ -Auswahl. Insbesondere gibt es stets $(q^k r^n, r)$ -H-Matrizen mit einer $q^k \cdot \rho q$ -Auswahl.

Beweis:

Das folgt unmittelbar aus 2.5.15 und 2.5.6.

2.5.17 Korollar

Es seien r und q Primzahlpotenzen, die (2.40) erfüllen.

Gilt dann $(s, q) \in \mathcal{RH}$, so gilt auch $(sr^n, r) \in \mathcal{RA}$. Insbesondere gilt stets $(q^k r^n, r) \in \mathcal{RH}$.

Beweis:

Das folgt unmittelbar aus 2.5.16 und 2.2.10.

2.5.18 Beispiele

Wir geben nun mit den früheren Methoden nicht erhaltbare Werte an:

r	2							
n	2	3		4				
q	9	17	19	27	29	31	37	41
sr ⁿ	4·9 ^k	8·17 ^k	8·19 ^k	16·27 ^k	16·29 ^k	16·31 ^k	16·37 ^k	16·41 ^k

r	2				3			
n	4		2		2			
q	43		9		16	17	19	
sr ⁿ	16·43 ^k	4·9·19 ^k	4·9·23 ^k	etc.	9·16 ^k	9·17 ^k	9·19 ^k	etc.

So erhalten wir zu den 25 nach 2.5.10 bekannten Paaren $(x, 2) \in \mathfrak{M}$ mit $x \leq 1000$ 14 weitere und zu den 48 bekannten Paaren $(x, 3) \in \mathfrak{M}$ mit $x \leq 1000$ die 9 weiteren Paare $(9q, 3)$ mit q Primzahlpotenz und $16 \leq q \leq 32$.

Die in 2.5.16 enthaltene Abschätzung (2.40) ist wesentlich schlechter als die Abschätzungen in Satz 2.1.5.(iii) und (iv), der - mit $\mathfrak{M}$ statt $\mathfrak{M}$ - Satz 2.5.16 entspricht. Mit der Methode von x-Auswahlen läßt sich jedoch nichts wesentlich Besseres als (2.40) erreichen, wie die folgende Größenordnungs-Abschätzung zeigt: Für eine (t, r) -H-Matrix mit x-Auswahl ist die Anzahl der Differenzen mit erstem Glied aus der Auswahl

$$(t-1)x(r+1) > t^{2-1}$$

(da alle Differenzen - wie in 2.5.5 beschrieben - jedes der t^{2-1} Elemente $\neq 0$ mindestens zweimal enthalten müssen), also $x \geq \frac{t+1}{r+1}$, für $t=r^n$ x somit in der Größenordnung von r^{n-1} .

2.5.19 Satz

α und r seien Primzahlpotenzen, die (2.40) erfüllen, und es gebe eine (s, α) -H-Matrix. q' sei eine weitere Primzahlpotenz mit

$$(2.41) \quad (s+\alpha+1)(r+1) \leq \alpha'+1 \leq r^n s(r+1),$$

wo pq wie in Satz 2.5.16 definiert ist. Wenn es eine

(s', q') -H-Matrix gibt, gibt es auch eine $(s' sr^n, r)$ -H-Matrix mit einer $s' \cdot \rho q'$ -Auswahl.

Beweis:

Das folgt unmittelbar aus 2.5.16 und 2.5.6.

2.5.20 Korollar

σ und r seien Primzahlpotenzen, die (2.40) erfüllen. Es sei $(s, q) \in \mathfrak{H}_1$. q' sei eine weitere Primzahlpotenz, die (2.41) erfüllt. Es sei $(s', q') \in \mathfrak{H}_1$. Dann ist auch $(s' sr^n, r) \in \mathfrak{H}_1$, insbesondere stets $(q'^k sr^n, r) \in \mathfrak{H}_1$.

Beweis:

Das folgt unmittelbar aus 2.5.19, 2.2.10 und 2.4.0.

2.5.21 Beispiele

Sei $r=2$, $n=3$ und $q=s=17$. Nach 2.5.20 erhalten wir $(8 \cdot 17 \cdot q'^k, 2) \in \mathfrak{H}_1$ für Primzahlpotenzen q' mit $308 \leq q' \leq 407$. Durch Kombination von 2.5.17 und 2.5.8 können wir die entsprechenden Parameter für $35 \leq q' \leq 305$ erhalten. Durch 2.5.20 ergeben sich also wieder PH-Ebenen mit bisher unbekannten Parametern. Die genauere Diskussion - analog zu der in 2.5.13 - sei dem Leser überlassen. Es ist wiederum klar, daß das Verfahren fortgesetzt werden kann.

3. LATEINISCHE QUADRATE UND TD'S

In diesem Kapitel konstruieren wir TD's mit abelscher, auf jeder Punktklasse regulärer und auf den Geraden semiregulärer Kollineationsgruppe sowie reguläre Sätze paarweise orthogonaler lateinischer Quadrate.

3.1 Grundlagen

3.1.1 Definition

Eine $t \times t$ - Matrix $A = (a_{ik})$ mit Einträgen aus einer t -elementigen Symbolmenge S heißt ein lateinisches Quadrat der Ordnung t , wenn gilt:

(LQ) In jeder Zeile und Spalte von A kommt jedes Element von S genau einmal vor.

Zwei lateinische Quadrate $A = (a_{ik})$, $B = (b_{ik})$ der Ordnung t auf der Symbolmenge S heißen orthogonal, wenn unter den Paaren (a_{ik}, b_{ik}) jedes Element von $S \times S$ genau einmal vorkommt.

Mit $N(t)$ bezeichnen wir die Maximalzahl paarweise orthogonaler lateinischer Quadrate der Ordnung t .

3.1.2 Satz

- (i) $N(t) \leq t-1$ für alle t .
- (ii) $N(t) = t-1$ genau dann, wenn es eine projektive Ebene der Ordnung t gibt.
- (iii) $N(t) = t-1$ für jede Primzahlpotenz t .
- (iv) $N(t_1, t_2) \geq \min \{N(t_1), N(t_2)\}$ (Satz von McNeish)
- (v) Wenn $t = q_1 \dots q_n$ die Primzahlpotenzzerlegung von t ist, gilt $N(t) \geq \min \{q_i - 1: i = 1, \dots, n\}$
- (vi) $N(t) \geq 2$ für $t \neq 2, 6$. $N(t) = 1$ für $t = 2, 6$.
(Satz von Bose-Shrikhande-Parker)
- (vii) $N(t) \geq 5$ für $t \geq 63$ (Satz von Harani)
- (viii) $N(t) \geq 6$ für $t \geq 91$ (Satz von Wilson)
- (ix) $\lim_{t \rightarrow \infty} N(t) = \infty$ (Satz von Chowla-Erdős-Straus)

Beweis:

HALL 1967, MC NETSH 1922, BOSE-SHRIKHANDE-PARKER 1960,
TARRY 1902, HANANI 1975, WILSON 1974a, CHOWLA-EPSTEIN-
STPAUS 1960.

3.1.3 Definition

$\Sigma = (\pi, \mathcal{L}, I)$ sei eine Inzidenzstruktur und π sei in $r \geq 3$
Punktklassen zerlegt. Σ heit ein (t, r) -TD ('transversal
design'), wenn gilt:

- (TD₁) Je zwei Punkte aus verschiedenen Punktklassen
sind eindeutig verbindbar.
- (TD₂) Jede Gerade enthlt genau einen Punkt aus
jeder Punktklasse. Ein Punkt ist auf genau t
Geraden.

Ein (t, r) -TD ist die duale Struktur eines (t, r) -Netzes
(vgl. BRUCK 1951, 1963).

3.1.4 Satz

Σ sei ein (t, r) -TD. Dann gilt:

- (i) Jeder Punkt von Σ ist auf t Geraden.
- (ii) Jede Gerade von Σ enthlt r Punkte.
- (iii) Jede Punktklasse enthlt t Punkte.
- (iv) Σ hat tr Punkte.
- (v) Σ hat t^2 Geraden.

Beweis:

BRUCK 1951, 1963.

3.1.5 Satz

Ein (t, r) -TD existiert genau dann, wenn es $r-2$ paarweise
orthogonale lateinische Quadrate der Ordnung t gibt.

Beweis:

WILSON 1967, S. 177-178.

3.2 Differenzenmatrizen und lateinische Quadrate

3.2.1 Definition

G sei eine abelsche Gruppe der Ordnung t und $D = (d_{ik})$ ($i=0, \dots, r; k=1, \dots, t$) eine $(r+1) \times t$ -Matrix mit Einträgen aus G , so daß gilt:

(DM) Für jedes Paar (i, j) mit $i \neq j$ und $i, j = 0, \dots, r$
ist $\{d_{i1}-d_{j1}, d_{i2}-d_{j2}, \dots, d_{it}-d_{jt}\} = G$,

d.h. die Differenz von je zwei Zeilen von D enthält jedes Element von G (aus Anzahlgründen genau einmal). Dann heißt D eine (t, r, G) -Differenzenmatrix.

Gilt überdies noch

$$(N\ 1) \quad d_{r1} = d_{r2} = \dots = d_{rt} = 0$$

$$(N\ 2) \quad d_{0t} = d_{1t} = \dots = d_{rt} = 0$$

heißt D normal.

3.2.2 Hilfssatz

D sei eine (t, r, G) -Differenzenmatrix und D' gehe aus D durch Operationen der folgenden Art hervor:

- (i) Zeilenpermutationen oder Spaltenpermutationen
 - (ii) Addition eines festen $a \in G$ zu einer Spalte von D
 - (iii) Addition eines festen $a \in G$ zu einer Zeile von D .
- Dann ist auch D' eine (t, r, G) -Differenzenmatrix.

Beweis:

Diese Operationen lassen Eigenschaft (DM) invariant.

3.2.3 Korollar

Zu jeder (t, r, G) -Differenzenmatrix D gibt es eine normale (t, r, G) -Differenzenmatrix D' , die aus D durch Operationen der in 3.2.2 beschriebenen Arten hervorgeht. D' erfüllt außerdem

- (N 3) Jede Zeile von D' (außer der letzten) enthält jedes Element von G genau einmal.

(N 4) Keine Spalte von D' (außer der letzten) enthält ein Element von G zweimal.

Beweis:

(N 1) kann durch Operationen des Typs (ii) und (N 2) durch solche des Typs (iii) erreicht werden. (N 3) gilt dann wegen (DM), da die Differenz zwischen der i -ten und der r -ten Zeile von D' wegen (N 1) einfach die i -te Zeile von D' ist. Auch (N 4) gilt nach (DM); denn da $d_{it} - d_{jt} = 0 - 0 = 0$ nach (N 2) gilt, muß $d_{ik} - d_{jk} \neq 0$ sein ($i \neq j$, $k \neq t$).

3.2.4 Beispiele

$G = \mathbb{Z}_3$, $r=2$ $G = \mathbb{Z}_5$, $r=4$ $G=EA(4)$, $r=3$, w erzeugendes Element von $GF(4)^*$

$$\begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 4 & 3 & 1 & 0 \\ 4 & 3 & 1 & 2 & 0 \\ 3 & 1 & 2 & 4 & 0 \\ 1 & 2 & 4 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} w & w^2 & 1 & 0 \\ w^2 & 1 & w & 0 \\ 1 & w & w^2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

3.2.5 Definition

Es sei $\mathfrak{u} = \{A_1, \dots, A_n\}$ mit $A_j = (a_{ik}^j)$ ($j=1, \dots, n$) eine Menge paarweise orthogonaler $t \times t$ -Matrizen auf der Symbolmenge $S = \{s_1, \dots, s_t\}$. G sei eine reguläre abelsche Permutationsgruppe auf S . Wenn es für jedes $\alpha \in G$ eine Permutation π der Zellen (i, k) gibt, so daß für jedes $j = 1, \dots, n$

$$(3.1) \quad (a_{ik}^j)^\alpha = a_{h1}^j \quad \text{mit} \quad (i, k)^\pi = (h, 1)$$

gilt, heißt $\mathfrak{u}$ G-quasiregulär. Wenn die Permutationen π sogar von der Form $(i, k) \mapsto (\sigma i, k)$ sind (wo σ eine Permutation von $\{1, \dots, t\}$ ist), heißt $\mathfrak{u}$ G-regulär.

$\mathfrak{u}$ heißt (quasi-)regulär, wenn es G -(quasi-)regulär für irgendeine Gruppe G ist.

3.2.6 Beispiel

Die folgenden 4 orthogonalen lateinischen Quadrate der Ord-

nung 5

$$\begin{pmatrix} 2 & 4 & 3 & 1 & 0 \\ 3 & 0 & 4 & 2 & 1 \\ 4 & 1 & 0 & 3 & 2 \\ 0 & 2 & 1 & 4 & 3 \\ 1 & 3 & 2 & 0 & 4 \end{pmatrix} \begin{pmatrix} 4 & 3 & 1 & 2 & 0 \\ 0 & 4 & 2 & 3 & 1 \\ 1 & 0 & 3 & 4 & 2 \\ 2 & 1 & 4 & 0 & 3 \\ 3 & 2 & 0 & 1 & 4 \end{pmatrix} \begin{pmatrix} 3 & 1 & 2 & 4 & 0 \\ 4 & 2 & 3 & 0 & 1 \\ 0 & 3 & 4 & 1 & 2 \\ 1 & 4 & 0 & 2 & 3 \\ 2 & 0 & 1 & 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 4 & 3 & 0 \\ 2 & 3 & 0 & 4 & 1 \\ 3 & 4 & 1 & 0 & 2 \\ 4 & 0 & 2 & 1 & 3 \\ 0 & 1 & 3 & 2 & 4 \end{pmatrix}$$

sind zusammen mit der Matrix

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 & 3 \\ 4 & 4 & 4 & 4 & 4 \end{pmatrix}$$

eine $\mathbb{Z}_5$ -reguläre Menge von 5 paarweise orthogonalen 5×5 -Matrizen. Ersetzen des Symboles $i \in \mathbb{Z}_5$ durch das Symbol $i+k \pmod{5}$ [$k \in \mathbb{Z}_5$] wird dabei durch die Permutation $\pi_k: (h,1) \mapsto (h+k,1) \pmod{5}$ dargestellt.

Die angegebenen lateinischen Quadrate sind aus der in 3.2.4 aufgeführten $(5,4, \mathbb{Z}_5)$ -Differenzenmatrix nach dem folgenden allgemeinen Satz hergestellt worden.

3.2.7 Satz

t und r seien natürliche Zahlen und G eine abelsche Gruppe der Ordnung t . Dann sind die folgenden Aussagen äquivalent:

- (i) Es gibt eine (t,r,G) -Differenzenmatrix.
- (ii) Es gibt eine G -reguläre Menge von $r+1$ paarweise orthogonalen $t \times t$ -Matrizen, von denen r lateinische Quadrate sind.
- (iii) Es gibt eine G -quasireguläre Menge von $r+1$ paarweise orthogonalen $t \times t$ -Matrizen, von denen r lateinische Quadrate sind.
- (iv) Es gibt eine G -quasireguläre Menge von $r+1$ paarweise orthogonalen $t \times t$ -Matrizen.
- (v) Es gibt eine G -reguläre Menge von r paarweise orthogonalen lateinischen Quadraten der Ordnung t .

Beweis:

I. (i) $\Rightarrow$ (ii)

Es sei $D = (d_{ik})$ eine (t, r, G) -Differenzenmatrix und $a_1 := 0$ sowie $a_2, \dots, a_t$ seien die Elemente von G . Für $i = 0, \dots, r$ definieren wir die $t \times t$ -Matrix $A_i = (a_{hk}^i)$ durch

$$(3.2) \quad a_{hk}^i := d_{ik} + a_h \quad (h, k = 1, \dots, t).$$

Die so definierten Matrizen sind paarweise orthogonal; seien nämlich $i, j \in \{0, \dots, r\}$ mit $i \neq j$ gegeben und sei $(x, y) \in G \times G$ beliebig. Wir setzen $d := x - y$. Nach (DM) besitzt d genau eine Darstellung $d = d_{ik} - d_{jk}$. Wir setzen $a_h := x - d_{ik}$. Dann folgt aus (3.2)

$$a_{hk}^i = d_{ik} + a_h = d_{ik} + x - d_{ik} = x$$

und

$$a_{hk}^j = d_{jk} + a_h = d_{jk} + x - d_{ik} = x + y - x = y.$$

Also gilt

$$\{(a_{hk}^i, a_{hk}^j) : h, k = 1, \dots, t\} = G \times G,$$

d.h. A_i und A_j sind orthogonal.

Für jedes $g \in G$ lassen wir g auf G durch

$$(3.3) \quad x^g := x + g \quad \text{für alle } x \in G$$

operieren. Dann operiert G also als reguläre Permutationsgruppe auf sich selbst. Wir behaupten, daß die oben definierten Matrizen A_i G -regulär sind; sei nämlich ein beliebiges Element von G gegeben, etwa $g = a_1$. Wir setzen $a_h := a_h + a_1$. Dann gilt

$$(a_{hk}^i)^g = (d_{ik} + a_h)^g = d_{ik} + a_h + a_1 = d_{ik} + a_{h'} = a_{h'k}^i,$$

d.h.

$$(a_{hk}^i)^g = a_{mn}^i \quad \text{mit } (m, n) = (h, k)^\pi := (h', k).$$

Schließlich bemerken wir, daß $A_0, \dots, A_{r-1}$ lateinische Quadrate sind (zu diesem Zweck nehmen wir o.B.d.A. an, daß D gemäß 3.2.3 normal ist). Man betrachte ein festes $i \neq r$. Nach (N 3) und weil G eine Gruppe ist, enthält jede Zeile von A_i jedes Element von G genau einmal. Da jede

Spalte von A_i die Form $d_{ik} + G$ hat, enthält auch jede Spalte von A_1 jedes Element von G genau einmal. Also ist A_1 ein lateinisches Quadrat.

II. (ii) $\Rightarrow$ (iii)
trivial

III. (iii) $\Rightarrow$ (iv)
trivial

IV. (iv) $\Rightarrow$ (i)

Es sei $\{A_0, \dots, A_r\}$ mit $A_i = (a_{hk}^i)$ eine G -quasireguläre Menge von paarweise orthogonalen $t \times t$ -Matrizen auf der Symbolmenge S . Da G regulär auf S operiert, können wir S und G identifizieren und S als abelsche Gruppe betrachten: Nach Wahl eines festen Elementes 0 von S identifizieren wir das Element $s \in S$ mit dem eindeutig bestimmten $\alpha_s \in G$ mit $\alpha_s 0 = s$. Die Permutationen in G nehmen dann die Form (3.3) an (wenn wir G additiv schreiben). $a_1 := 0$ und $a_2, \dots, a_t$ seien die Elemente von S bzw. G . Da jede G -quasireguläre Menge von paarweise orthogonalen Matrizen offenbar durch jede Zellen-Permutation wieder in eine G -quasireguläre Menge von derartigen Matrizen übergeht, können wir o.B.d.A. annehmen, daß

$$a_{11}^r = a_{12}^r = \dots = a_{1t}^r = 0$$

und

$$a_{hk}^i = a_{1k}^i + a_h \quad \text{für } i=0, \dots, r$$

gelten. Wir definieren nun die $(r+1) \times t$ -Matrix $D = (d_{ik})$ durch

$$(3.4) \quad d_{ik} := a_{1k}^i \quad (i=0, \dots, r; k=1, \dots, t).$$

Man betrachte die Zeilen i und j ($i \neq j$) von D . Da A_i und A_j orthogonal sind, erscheint das Paar $(x, 0) \in G \times G$ (genau einmal) in der Form (a_{hk}^i, a_{hk}^j) . Nach (3.4) gilt daher

$$x = a_{hk}^i = a_{1k}^i + a_h = d_{ik} + a_h$$

und

$$0 = a_{hk}^j = a_{1k}^j + a_h = d_{jk} + a_h,$$

d.h. es gilt $x = x - 0 = d_{ik} - d_{jk}$. Die Differenz der i-ten und j-ten Zeile von D enthält also jedes Element von G (genau einmal), d.h. D ist eine (t, r, G) -Differenzenmatrix.

V. (ii) $\Rightarrow$ (v)

trivial

VI. (v) $\Rightarrow$ (ii)

$\{A_0, \dots, A_{r-1}\}$ mit $A_i = (a_{hk}^i)$ sei eine G-reguläre Menge von paarweise orthogonalen lateinischen Quadraten der Ordnung t. Wir definieren die $t \times t$ -Matrix $A_r = (a_{hk}^r)$ durch

$$a_{h1}^r = a_{h2}^r = \dots = a_{ht}^r := a_{it}^0.$$

Da $A_0, \dots, A_{r-1}$ lateinische Quadrate sind, ist $\{A_0, \dots, A_r\}$ offenbar eine Menge von paarweise orthogonalen $t \times t$ -Matrizen, von denen r lateinische Quadrate sind. Wir müssen noch zeigen, daß diese Menge G-regulär ist. Sei ein beliebiges $a \in G$ gegeben. Wir betrachten die Matrix $(A_r)^a = (a_{ik}^r + a)$. Das Element in der h-ten Zeile von A_r sei $b := a_{ht}^0$. π sei die zu a nach (3.1) gehörende Zeilenpermutation. Wenn π Zeile h in Zeile k abbildet, folgt $a_{kt}^0 = a_{ht}^0 + a = b + a$, d.h. Anwendung von π auf A_r bedeutet - genauso wie Anwendung von π auf jedes der übrigen A_i - Addition von a. Daher ist die Menge $\{A_0, \dots, A_r\}$ G-regulär.

3.3 Differenzenmatrizen und TD's

3.3.1 Definition

G sei eine abelsche Gruppe und Σ ein TD. Σ heißt G-regulär, wenn G als eine auf jeder Punktklasse von Σ reguläre und auf der Geradenmenge von Σ semireguläre Kollineationsgruppe von Σ wirkt.

3.3.2 Satz

D sei eine (t, r, G) -Differenzenmatrix mit $r \geq 2$. Wir definieren eine Inzidenzstruktur $\Sigma = (\mathcal{P}, \mathcal{B}, \epsilon)$ durch

$$\mathcal{P} := \{(i, x) : i=0, \dots, r, x \in G\},$$

$$\mathcal{B} := \{G_i^x : i=1, \dots, t; x \in G\}$$

mit

$$G_i^x := \{(0, d_{0i}+x), (1, d_{1i}+x), \dots, (r, d_{ri}+x)\}.$$

Dann ist Σ ein G -reguläres $(t, r+1)$ -TD.

Umgekehrt läßt sich jedes G -reguläre $(t, r+1)$ -TD in dieser Form beschreiben.

Beweis:

' $\Rightarrow$ '

Es sei D eine (t, r, G) -Differenzenmatrix und Σ wie oben definiert. Offenbar sind Punkte der Form (i, x) und (i, x') stets unverbindbar. Wir betrachten nun Punkte (i, x) und (j, y) mit $i \neq j$. Da D eine Differenzenmatrix ist, gibt es genau einen Index k mit $d_{ik} - d_{jk} = x - y$. Dann gilt

$$(i, x) = (i, d_{ik} + (x - d_{ik})) \in G_k^{x - d_{ik}}$$

und

$$(j, y) = (j, d_{jk} + (y - d_{jk})) = (j, d_{jk} + (x - d_{ik})) \in G_k^{x - d_{ik}},$$

d.h. (i, x) und (j, y) sind verbindbar. Sei nun etwa $(i, x), (j, y) \in G_1^u$. Es folgt $d_{i1} + u = x$, $d_{j1} + u = y$, also $d_{i1} - d_{j1} = x - y$ und wegen (DM) $l=k$, $u=x-d_{ik}$ und somit die Eindeutigkeit der Verbindungsgeraden.

Σ ist also offenbar ein $(t, r+1)$ -TD mit Punktklassen

$$\mathcal{P}_i := \{(i, x) : x \in G\}. \text{ Offenbar bilden die Abbildungen}$$

$\tau_a : (i, x) \mapsto (i, x+a)$ für alle $x \in G$ und $i=0, \dots, r$ eine zu G isomorphe abelsche Kollineationsgruppe von Σ , die die gewünschten Regularitäts-Eigenschaften besitzt (τ_a wirkt auf $\mathcal{B}$ durch $\tau_a : G_i^x \mapsto G_i^{x+a}$).

' $\Leftarrow$ '

Sei nun Σ ein G -reguläres $(t, r+1)$ -TD. Wir indizieren die Punktklassen von Σ in willkürlicher Weise als $\mathcal{P}_1, \dots, \mathcal{P}_r$.

Wir wählen in jeder Klasse $\mathbb{P}_i$ willkürlich einen Basispunkt $p_i =: (i, 0)$. Der Punkt q , der sich aus $(i, 0)$ durch Anwendung der Kollineation x ergibt, erhält dann die Koordinaten (i, x) , was wegen der Regularität von G wohldefiniert ist. Nach Voraussetzung operiert G auf jedem Geradenorbit treu; es gibt also t derartige Orbits. Wir wählen in jedem dieser Orbits eine Startgerade $G_j^0 = \{(0, d_{0j}), (1, d_{1j}), \dots, (r, d_{rj})\}$. Jede Gerade ist dann in der Form G_j^x beschreibbar, wie oben angegeben. Wir setzen $D := (d_{ik})$ ($i=0, \dots, r; k=1, \dots, t$). Seien i, j mit $i \neq j$ gegeben. Nach Voraussetzung sind die Punkte (i, x) und $(k, 0)$ eindeutig verbindbar, etwa durch G_1^u . Es folgt $d_{i1} + u = x$, $d_{j1} + u = 0$, also $x = x - 0 = d_{i1} - d_{j1}$. Daher enthält die Differenz der Zeilen i und j von D jedes Element von G (aus Anzahlgründen genau einmal). Also ist D eine (t, r, G) -Differenzenmatrix und Σ läßt sich offenbar wie in der Behauptung beschrieben durch D darstellen.

3.3.3 Korollar

Es gibt eine $(12, 5, \mathbb{Z}_2 \oplus \mathbb{Z}_6)$ -Differenzenmatrix.

Beweis:

HANANI 1975, Lemma 3.21 gibt ein $(12, 6)$ -TD an, das offenbar $\mathbb{Z}_2 \oplus \mathbb{Z}_6$ -regulär ist.

3.3.4 Satz

Eine $(t, t-1, G)$ -Differenzenmatrix mit $t \geq 3$ existiert genau dann, wenn es eine projektive Ebene der Ordnung t gibt, die für eine geeignete Fahne (p, L) (p, L) -transitiv ist und G als die Elationsgruppe $G_{(p, L)}$ besitzt.

Beweis:

' $\Rightarrow$ '

Es sei D eine $(t, t-1, G)$ -Differenzenmatrix. Σ sei das in 3.3.2 konstruierte G -reguläre (t, t) -TD. Wir zerlegen die Geradenmenge $\mathfrak{B}$ in disjunkte Teilmengen $\mathfrak{B}_1, \dots, \mathfrak{B}_t$ mit

$$\mathfrak{B}_i := \{G_i^x : x \in G\} \quad \text{für } i=1, \dots, t.$$

Offenbar bilden die $\mathfrak{P}_i$ Parallelklassen von Σ . Adjungiert man zu jeder Geraden G_i^x den Punkt ω_i , so erhält man daher ein $(t, t+1)$ -TD Σ' , also eine dual-affine Ebene der Ordnung t , mit der weiteren Punktklasse $\mathfrak{P}_t = \{\omega_1, \dots, \omega_t\}$. Schließlich ernennen wir die Punktklassen $\mathfrak{P}_i$ ($i=0, \dots, t$) zu neuen Geraden:

$$G_0^i := \mathfrak{P}_i \quad \text{für } i=0, \dots, t$$

und erhalten eine weitere Parallelklasse $\mathfrak{P}_0$, zu der wir den neuen Punkt ω_0 hinzufügen. Insgesamt ergibt sich eine Inzidenzstruktur Σ'' , in der je zwei Punkte verbindbar sind, jede Gerade $t+1$ Punkte besitzt und die insgesamt t^2+t+1 Punkte enthält. Also ist Σ'' eine projektive Ebene der Ordnung t (vgl. CORSI 1964 oder DEMBOWSKI 1967 p.138-139). Man sieht sofort (aufgrund der Regularitätsvoraussetzungen über G), daß Σ'' (ω_0, G_0^t)-transitiv ist und die entsprechende Elationsgruppe isomorph zu G ist.

' $\Leftarrow$ '

Sei umgekehrt die projektive Ebene Π der Ordnung t (p, L)-transitiv ($p \in L$) und $G_{(p, L)} \cong G$. Wir entfernen aus Π die Gerade L mit allen mit ihr inzidenten Punkten und die verbleibenden t Geraden durch p , die wir als Punktklassen auffassen. Es entsteht ein bezüglich G reguläres (t, t) -TD Σ . Die Behauptung folgt daher aus Satz 3.3.2.

3.3.5 Korollar

Es sei t eine natürliche Zahl ≥ 3 und G eine abelsche Gruppe der Ordnung t . Dann sind die folgenden Aussagen äquivalent:

- (i) Es gibt eine G -reguläre Menge von $t-1$ paarweise orthogonal lateinischen Quadraten der Ordnung t .
- (ii) Es gibt ein G -reguläres (t, t) -TD.
- (iii) Es gibt eine (p, L) -transitive projektive Ebene der Ordnung t ($p \in L$ geeignet) mit $G_{(p, L)} \cong G$.
- (iv) Es gibt eine $(t, t-1, G)$ -Differenzenmatrix.

Beweis:

Das folgt unmittelbar aus 3.3.2, 3.3.4 und 3.2.7.

3.3.5 zeigt, daß die Regularität von TD's bzw. lateinischen Quadraten sowie die Existenz von Differenzenmatrizen in gewisser Hinsicht Verallgemeinerungen des Begriffes der (p,L) -Transitivität aus der Theorie der projektiven Ebenen sind.

Wir werden im nächsten Abschnitt Differenzenmatrizen konstruieren und uns danach nochmals mit den Kollineationen der korrespondierenden TD's beschäftigen.

3.4 Konstruktion von Differenzenmatrizen

3.4.1 Satz

t sei eine Primzahlpotenz. Dann gibt es für jedes $r \leq t-1$ eine $(t,r,EA(t))$ -Differenzenmatrix.

Beweis:

Man beachte, daß es wegen (N 4) für $r \geq t$ keine $(t,r,EA(t))$ -Differenzenmatrix geben kann. Wir betrachten $EA(t)$ als additive Gruppe des Körpers $F := GF(t)$. w sei erzeugendes Element von F^* . Wir definieren die $(r+1) \times t$ -Matrix

$D = (d_{ik})$ ($i=0, \dots, r$; $k=1, \dots, t$) durch

$$d_{ik} := \begin{cases} 0 & \text{für } i=r \text{ oder } k=t \\ w^{i+k} & \text{sonst} \end{cases}$$

und erhalten also

$$D = \begin{pmatrix} w & w^2 & w^3 & \dots & w^{t-1} & 0 \\ w^2 & w^3 & w^4 & \dots & w^t & 0 \\ \vdots & & & & & \vdots \\ w^r & w^{r+1} & w^{r+2} & \dots & w^{t+r-2} & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}.$$

(Man beachte $w^{t-1} = 1$).

Wir müssen zeigen, daß D Eigenschaft (DM) aus 3.2.1 erfüllt. Wir betrachten zunächst die Zeilen r und i ($i \neq r$). Ihre Differenz ergibt einfach die i -te Zeile selbst, die jedes Element von F genau einmal enthält, da sie aus der

Zeile 0 durch Multiplikation mit $w^i \neq 0$ hervorgeht und diese Zeile jedes Element von F genau einmal enthält, da w erzeugendes Element ist.

Wir betrachten nun die Zeilen i und j ($i \neq j$, $i, j \neq r$). Als Differenz ergibt sich

$$\begin{aligned} & \{w^{i+1}-w^{j+1}, w^{i+2}-w^{j+2}, \dots, w^{i+t-1}-w^{j+t-1}, 0-0\} \\ &= (1-w^{j-i})\{w^{i+1}, w^{i+2}, \dots, w^{i+t-1}, 0\}; \end{aligned}$$

dies sind aber alle Elemente von F , da $1-w^{j-i} \neq 0$ ist und F ein Körper ist.

Diese Konstruktion findet sich in äquivalenter Form bereits bei BOSE 1938.

3.4.2 Satz

Es sei $t=p^n$ eine Primzahlpotenz und $r \leq p-1$. Dann existiert eine $(t, r, \mathbb{Z}_t)$ -Differenzenmatrix.

Beweis:

Man definiere die $(r+1) \times t$ -Matrix $D = (d_{ik})$ ($i=0, \dots, r$; $k=1, \dots, t$) durch

$$d_{ik} := \begin{cases} 0 & \text{für } i=r \text{ oder } k=t \\ (i+1)k & \text{sonst} \end{cases}$$

(alles mod p^n) und erhält also

$$D = \begin{pmatrix} 1 & 2 & 3 & \dots & p^{n-1} & 0 \\ 2 & 4 & 6 & \dots & 2(p^{n-1}) & 0 \\ \vdots & & & & & \vdots \\ r & 2r & 3r & \dots & r(p^{n-1}) & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}.$$

Da $1, \dots, r$ sowie die Differenzen $x-y$ ($x \neq y$, $x, y = 1, \dots, r$) sämtlich Einheiten des Rings $\mathbb{Z}_t$ sind, zeigt man leicht (mit Argumenten, die den in 3.4.1 benutzen analog sind), daß D eine Differenzenmatrix ist.

3.4.3 Satz

Wenn es eine (t, r, G) - und eine (t', r, G') -Differenzenmatrix gibt, gibt es auch eine $(tt', r, G \otimes G')$ -Differenzenmatrix.

Beweis:

Es sei $D = (d_{ik})$ mit $i=0, \dots, r$ und $k=1, \dots, t$ eine (t, r, G) -Differenzenmatrix und $D' = (d'_{ik})$ mit $i=0, \dots, r$ und $k=1, \dots, t'$ eine (t', r, G') -Differenzenmatrix. Wir definieren eine $(r+1) \times tt'$ -Matrix D'' über $G \otimes G'$ durch

$$d''_{ik} := (d_{i, \alpha k}, d'_{i, k - (\alpha k - 1)t'}) \quad (i=0, \dots, r; k=1, \dots, tt'),$$

wobei αk die kleinste ganze Zahl $\geq \frac{k}{t'}$ bezeichnet. Wir erhalten also

$$D'' = \begin{pmatrix} (d_{01}, d'_{01}) \dots (d_{01}, d'_{0t'}) \dots (d_{0t}, d'_{01}) \dots (d_{0t}, d'_{0t'}) \\ \vdots \\ (d_{r1}, d'_{r1}) \dots (d_{r1}, d'_{rt'}) \dots (d_{rt}, d'_{r1}) \dots (d_{rt}, d'_{rt'}) \end{pmatrix}.$$

D'' erfüllt (DM): Sei nämlich $d''_{ik} - d''_{jk} = d''_{i1} - d''_{j1}$ ($i \neq j$).

Dann folgt

$$d_{i, \alpha k} - d_{j, \alpha k} = d_{i, \alpha 1} - d_{j, \alpha 1}$$

und

$$\begin{aligned} d'_{i, k - (\alpha k - 1)t'} - d'_{j, k - (\alpha k - 1)t'} \\ = d'_{i, 1 - (\alpha 1 - 1)t'} - d'_{j, 1 - (\alpha 1 - 1)t'}. \end{aligned}$$

Da D eine Differenzenmatrix ist, folgt $\alpha k = \alpha 1$. Da D' eine Differenzenmatrix ist, folgt $k - (\alpha k - 1)t' = 1 - (\alpha 1 - 1)t'$. Aus beiden Bedingungen zusammen ergibt sich sofort $k=1$. Also ist D'' eine Differenzenmatrix. Wenn D und D' normal sind, ist es offenbar auch D'' .

3.4.4 Beispiel

Wir betrachten die folgenden Differenzenmatrizen über $\mathbb{Z}_3$ bzw. $\mathbb{Z}_5$ ($r=2$):

$$\begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 2 & 4 & 3 & 1 & 0 \\ 4 & 3 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Die Konstruktion in 3.4.3 ergibt die folgende Differenzenmatrix über $\mathbb{Z}_{15} = \mathbb{Z}_3 \oplus \mathbb{Z}_5$ (wir schreiben xy statt (x,y)):

$$\begin{pmatrix} 22 & 24 & 23 & 21 & 20 & 12 & 14 & 13 & 11 & 10 & 02 & 04 & 03 & 01 & 00 \\ 14 & 13 & 11 & 12 & 10 & 24 & 23 & 21 & 22 & 20 & 04 & 03 & 01 & 02 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \end{pmatrix}$$

3.4.5 Korollar

Es sei $t = q_1 \dots q_n$, q_i Primzahlpotenz und $r \leq q_i - 1$ für $i=1, \dots, n$. Dann gibt es eine $(t, r, \text{EA}(q_1) \oplus \dots \oplus \text{EA}(q_n))$ -Differenzenmatrix.

Beweis:

Das folgt unmittelbar aus 3.4.1 und 3.4.3.

3.4.6 Korollar

Es sei $t = p^n$ Primzahlpotenz und G eine beliebige abelsche Gruppe der Ordnung t . Wenn G elementar-abelsch ist, gibt es genau für die Werte von r mit $0 \leq r \leq t-1$ (t, r, G) -Differenzenmatrizen, sonst für mindestens die Werte mit $0 \leq r \leq p-1$.

Beweis:

Bekanntlich ist G direkte Summe zyklischer p -Gruppen (siehe z.B. HALL 1959 p.40-41). Daher folgt die Behauptung unmittelbar aus 3.4.1, 3.4.2 und 3.4.3.

3.4.7 Korollar

G sei eine beliebige abelsche Gruppe der Ordnung t und $t = q_1 \dots q_n$ mit $q_i = p_i^{e_i}$ für $i=1, \dots, n$ die Primzahlpotenzzerlegung von t . Es sei $p := \min \{p_1, \dots, p_n\}$ und $q := \min \{q_1, \dots, q_n\}$. Bekanntlich ist G direkte Summe von zyklischen p_i -Gruppen ($i=1, \dots, n$) (siehe etwa HALL 1959 p.40-41). Wenn alle diese Gruppen elementar-abelsch sind, gibt es (t, r, G) -Differenzenmatrizen mindestens für $0 \leq r \leq q-1$, sonst für mindestens $0 \leq r \leq p-1$.

3.4.8 Satz

Es sei $t = 2n$ mit $(n, 2) = 1$. Dann gibt es keine $(t, 2, G)$ -Differenzenmatrizen (G beliebig).

Beweis:

Angenommen, D wäre eine $(t, 2, G)$ -Differenzenmatrix, nach 3.2.3 o.B.d.A. normal. Da $(2, n) = 1$ gilt, gibt es eine Zerlegung $G = \mathbb{Z}_2 \oplus G'$ (z.B. HALL 1959, p.40-41). Die Elemente von G haben also die Form $(0, x)$ bzw. $(1, x)$ mit $x \in G'$. Wir betrachten die Differenzen zwischen der 0-ten und 1-ten Zeile von D . n dieser Differenzen müssen die Form $(0, x)$, die restlichen n die Form $(1, x)$ haben. Angenommen, es stehen u Elemente der Form $(0, x)$ unter u Elementen der Form $(0, x')$. Das gibt dann u Differenzen mit erster Koordinate 0; um die verbleibenden $n-u$ Differenzen dieser Form zu erhalten, müssen also $n-u$ Elemente der Form $(1, x)$ unter $n-u$ Elementen der Form $(1, x')$ stehen. Da D normal ist, enthalten aber die ersten beiden Zeilen je alle Elemente aus G . Daher müssen die noch verbleibenden $n-u$ Elemente der Form $(0, x)$ in Zeile 1 unter den noch verbleibenden u Elementen der Form $(1, x')$ in Zeile 0 stehen. Es folgt $n-u = u$, d.h. $n = 2u$ im Widerspruch zu $(n, 2) = 1$. Es kann also keine $(t, 2, G)$ -Differenzenmatrix geben.

3.4.9 Korollar

Die Klasse der regulären lateinischen Quadrate erfüllt die Eulersche Vermutung: wenn $t \equiv 2 \pmod{4}$ ist, gibt es keine reguläre Menge von 2 orthogonalen lateinischen Quadraten.

Beweis:

Das folgt unmittelbar aus 3.4.8 und 3.2.7.

3.4.9 zeigt, daß die Klasse RLQ der regulären Mengen von paarweise orthogonalen lateinischen Quadraten eine echte Unterklasse der Klasse LQ von paarweise orthogonalen lateinischen Quadraten ist, da für LQ die Eulersche Vermu-

tung durch BOSE-SHRIKHANDE 1959 widerlegt wurde (vgl. Satz 3.1.2.(vi)).

3.4.5 zeigt, daß die Klasse RLQ den Satz von McNeish, wie er für LQ bekannt ist, erfüllt (vgl. Satz 3.1.2.(iv) und (v)). McNeish stellte in seiner Arbeit 1922 die Vermutung auf, daß die von ihm gefundene untere Grenze für $N(t)$ schon den exakten Wert darstellen würde (das also 3.1.2.(iv) und (v) mit $=$ statt $\geq$ gelten). Da dies die Gültigkeit der Eulerschen Vermutung beinhaltet, wurde es mit dieser zusammen widerlegt. Da aber die Klasse RLQ die Eulersche Vermutung erfüllt, scheint es vorstellbar, daß sie sogar die McNeishsche Vermutung erfüllt. Daß das nicht der Fall ist, zeigt die folgende Konstruktion.

3.4.10 Satz

Es sei q eine Primzahlpotenz und $v := q^2 + q + 1$. Dann gibt es für jedes $r \leq N(q+1)$ eine $(v, r, \mathbb{Z}_v)$ -Differenzenmatrix.

Beweis:

Da q eine Primzahlpotenz ist, gibt es nach dem Satz von SINGER 1938 eine Differenzenmenge $\{a_0, \dots, a_q\}$ in $\mathbb{Z}_v$. Nach Voraussetzung gibt es eine Menge $\{D_1, \dots, D_r\}$ von paarweise orthogonalen lateinischen Quadraten der Ordnung $q+1$ (o.B.d.A. auf den Symbolen $0, \dots, q$; ferner mögen alle Quadrate als erste Zeile $0, \dots, q$ haben (vgl. z.B. HALL 1959 p. 189-190)). D_0 sei die $(q+1) \times (q+1)$ -Matrix mit allen Zeilen $0, \dots, q$. Mit $\vec{d}_k^i$ bezeichnen wir die k -te Zeile von D_i . Wir bilden die Matrix

$$D' := \begin{pmatrix} \vec{d}_1^0 & \dots & \vec{d}_q^0 \\ \vdots & & \vdots \\ \vec{d}_1^r & \dots & \vec{d}_q^r \end{pmatrix}$$

und erhalten daraus die $(r+1) \times (q(q+1)+1)$ -Matrix D , indem wir in D' jedes Element i durch a_i ersetzen ($i=0, \dots, q$) und eine Spalten mit allen Einträgen 0 hinzufügen. Das so definierte D ist eine $(v, r, \mathbb{Z}_v)$ -Differenzenmatrix. Man betrachte

nämlich die Reihen i und j von D ($i \neq j$). Da D_i und D_k orthogonal sind, kommt nach Konstruktion jedes Paar (k, l) mit $k \neq l$ und $k, l = 0, \dots, q$ in der i -ten und j -ten Zeile von D' in genau einer Spalte vor. Also kommt in D in der i -ten und j -ten Zeile jede Differenz $a_k - a_l$ ($k \neq l$) genau einmal vor. Da $\{a_0, \dots, a_r\}$ eine Differenzenmenge ist, kommt also jedes Element $\neq 0$ von $\mathbb{Z}_v$ genau einmal vor; schließlich kommt die Differenz 0 genau in der letzten Spalte von D vor.

3.4.11 Beispiel

Zum besseren Verständnis der Konstruktion in 3.4.10 betrachten wir das folgende Beispiel für $r=q=4$. Zunächst erhalten wir aus den in 3.2.6 angegebenen lateinischen Quadraten der Ordnung 5 die folgenden Quadrate mit erster Zeile $0, 1, 2, 3, 4$:

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \end{pmatrix},$$

woraus sich mit der Differenzenmenge $\{3, 6, 12, 7, 14\}$ von $\mathbb{Z}_{21}$ die folgende $(21, 4)$ -Differenzenmatrix ergibt:

$$\begin{pmatrix} 3 & 6 & 12 & 7 & 14 & 3 & 6 & 12 & 7 & 14 & 3 & 6 & 12 & 7 & 14 & 3 & 6 & 12 & 7 & 14 & 0 \\ 6 & 12 & 7 & 14 & 3 & 7 & 14 & 3 & 6 & 12 & 14 & 3 & 6 & 12 & 7 & 12 & 7 & 14 & 3 & 6 & 0 \\ 12 & 7 & 14 & 3 & 6 & 6 & 12 & 7 & 14 & 3 & 7 & 14 & 3 & 6 & 12 & 14 & 3 & 6 & 12 & 7 & 0 \\ 14 & 3 & 6 & 12 & 7 & 12 & 7 & 14 & 3 & 6 & 6 & 12 & 7 & 14 & 3 & 7 & 14 & 3 & 6 & 12 & 0 \\ 7 & 14 & 3 & 6 & 12 & 14 & 3 & 6 & 12 & 7 & 12 & 7 & 14 & 3 & 6 & 6 & 12 & 7 & 14 & 3 & 0 \end{pmatrix}$$

und schließlich nach Normalisierung gemäß 3.2.3:

$$\begin{pmatrix} 17 & 13 & 9 & 1 & 2 & 10 & 3 & 6 & 16 & 7 & 12 & 20 & 19 & 4 & 8 & 18 & 15 & 5 & 14 & 11 & 0 \\ 20 & 19 & 4 & 8 & 12 & 14 & 11 & 18 & 15 & 5 & 2 & 17 & 13 & 9 & 1 & 6 & 16 & 7 & 10 & 3 & 0 \\ 5 & 14 & 11 & 18 & 15 & 13 & 9 & 1 & 2 & 17 & 16 & 7 & 10 & 3 & 6 & 8 & 12 & 20 & 19 & 4 & 0 \\ 7 & 10 & 3 & 6 & 16 & 19 & 4 & 8 & 12 & 20 & 15 & 5 & 14 & 11 & 18 & 1 & 2 & 17 & 13 & 9 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Weiter geben wir die folgenden Beispiele an (nur Werte, die nicht schon nach 3.4.7 bekannt sind; s gibt den nach 3.4.7 bekannten Wert an):

q .	4	7	16	19	31	49	61	67
q+1	5	8	17	20	32	50	62	68
r	4	7	16	3	31	6*)	4+)	5+)
v	21	57	273	381	993	2451	3783	4557
s	2	2	2	2	2	2	2	etc.

+) LINT 1974 *) WILSON 1974c

3.4.12 Satz

q sei Primzahlpotenz und es existiere eine $(q-1, r, \mathbb{Z}_{q-1})$ -Differenzenmatrix. Dann existiert auch eine $(q^2-1, r, \mathbb{Z}_{q^2-1})$ -Differenzenmatrix.

Beweis:

Da q eine Primzahlpotenz ist, gibt es eine affine Differenzenmenge in $\mathbb{Z}_{q^2-1}$, etwa $\{a_1, \dots, a_q\}$ (vgl. BOSE 1942, HOFFMANN 1952, DEMBOWSKI 1967 p. 210-211), d.h. unter den Differenzen $a_i - a_j$ ($i \neq j$, $i, j = 1, \dots, q$) kommt jedes Element aus $\mathbb{Z}_{q^2-1}$, das $\not\equiv 0 \pmod{q+1}$ ist (also alle Elemente außer 0, $q+1$, ..., $(q-2)(q+1)$) genau einmal vor. Die nicht auftretenden Elemente bilden also eine zyklische Gruppe $\{b_0, \dots, b_{q-2}\} \cong \mathbb{Z}_{q-1}$.

Wegen $(N \ 4)$ gilt $r \leq q-2$, also gibt es $r+1$ paarweise orthogonale lateinische Quadrate der Ordnung q, etwa $D_0, \dots, D_r$ (o.B.d.A. auf den Symbolen $\{1, \dots, q\}$ und alle mit erster Zeile $1, \dots, q$). Wir bezeichnen wieder die k-te Zeile von D_i mit $\vec{d}_k^i$. Wir bilden die Matrix

$$A := \begin{pmatrix} \vec{d}_2^0 & \dots & \vec{d}_q^0 \\ \vdots & & \vdots \\ \vec{d}_2^r & \dots & \vec{d}_q^r \end{pmatrix}$$

und erhalten daraus durch Ersetzen jedes Elements i durch a_i eine $(r+1) \times q(q-1)$ -Matrix A' , für die die Differenz von je zwei verschiedenen Zeilen alle Elemente aus $\mathbb{Z}_{q^2-1}$ außer $\{b_0, \dots, b_{q-2}\}$ enthält. Sei nun B eine $(q-1, r, \mathbb{Z}_{q-1})$ -Differenzenmatrix. Wir ersetzen in B jedes Element i durch das Element b_i und erhalten eine $(r+1) \times (q-1)$ -Matrix B' , für die die Differenz von je zwei verschiedenen Zeilen

gerade die Elemente $b_0, \dots, b_{q-2}$ enthält. Daher ist

$$D := (A' \ B')$$

eine $(q^2-1, r, \mathbb{Z}_{q^2-1})$ -Differenzenmatrix.

3.4.13 Beispiele

Wir geben nur Beispiele, die nicht schon nach 3.4.7 bekannt sind (s gibt den nach 3.4.7 bekannten Wert an):

q	8	32	128	512	2048	
q-1	7	31	127	511	2047	
r	6	30	126	6	22	
q^2-1	63	1023	129·127	511·513	2047·2049	
s	2	2	2	2	2	etc.

Soweit uns bekannt ist, haben wir damit (gemäß 3.2.7) für $t = 31 \cdot 33$, $127 \cdot 129$ und $2047 \cdot 2049$ neue untere Schranken für $N(t)$ gefunden, nämlich 30, 126 bzw. 22. Nach dem Satz von McNeish würde jeweils nur $N(t) \geq 2$ folgen (3.1.2.(v)) bzw. nach dem Satz von Wilson $N(t) \geq 6$ (3.1.2.(viii)).

3.4.14 Satz

D sei die in 3.4.1 konstruierte $(t, r, EA(t))$ -Differenzenmatrix und Σ das in 3.3.2 konstruierte $EA(t)$ -reguläre $(t, r+1)$ -TD. Wir bezeichnen mit $\mathfrak{N}$ die Gruppe der Kollineationen τ_a von Σ (wie im Beweis von 3.3.2). Dann bilden die Abbildungen $\pi_i: (1, x) \mapsto (1, xw^i)$ ($i=0, \dots, r$; $x \in EA(t)$) eine zu $\mathbb{Z}_{t-1}$ isomorphe Kollineationsgruppe $\mathfrak{M}$ von Σ . $\mathfrak{U}$ sei die von $\mathfrak{M}$ und $\mathfrak{N}$ erzeugte Kollineationsgruppe von Σ . Dann gilt:

- (i) $\mathfrak{U}$ ist das halbdirekte Produkt von $\mathfrak{N}$ mit $\mathfrak{M}$.
- (ii) $\mathfrak{U}$ ist auf jeder Punktklasse scharf zweifach transitiv.
- (iii) Die Geradenmenge $\{G_i^x: i=1, \dots, t-1; x \in EA(t)\}$ ist ein Orbit, auf dem $\mathfrak{U}$ treu operiert.

Beweis:

π_i ist eine Kollineation, denn es gilt

$$\pi_i: \begin{cases} G_j^x \rightarrow G_{j+i}^{xw_i^1} \\ G_t^x \rightarrow G_t^{xw_i^1} \end{cases} \quad (j=1, \dots, t-1; x \in EA(t))$$

(Indizes mod $t-1$). Daß $\mathfrak{M}$ eine Gruppe $\cong \mathbb{Z}_{t-1}$ ist, ist klar.

(i) Wegen

$$(k, x) \pi_i \tau_a \pi_i^{-1} = (k, xw_i^1 + a) \pi_i^{-1} = (k, x + aw^{-i})$$

gilt $\pi_i \tau_a \pi_i^{-1} = \tau_{aw^{-i}}$. Also ist $\mathfrak{M}$ Normalteiler von $\mathfrak{U}$. Offenbar ist $\mathfrak{M}$ Untergruppe von $\mathfrak{U}$ und $\mathfrak{M} \cap \mathfrak{N} = 1$. Also ist $\mathfrak{U}$ das halbdirekte Produkt von $\mathfrak{N}$ mit $\mathfrak{M}$ (siehe z.B. HALL 1959 Theorem 6.5.3). $\mathfrak{U}$ ist offenbar nicht abelsch, also kein direktes Produkt.

(ii) Offenbar ist $\mathfrak{M}$ der Stabilisator des Punktes $(i, 0)$ in $\mathfrak{U}$; ferner ist $\mathfrak{M}$ auf den übrigen Punkten (i, x) transitiv. Also ist $\mathfrak{U}$ auf allen Punkten der Form (i, x) zweifach transitiv (siehe z.B. WIELANDT 1964 Theorem 9.1). Aus Anzahlgründen ist $\mathfrak{U}$ scharf zweifach transitiv.

(iii) Das folgt bereits aus den am Anfang des Beweises gegebenen Argumenten (Wirkung von π_i auf G_j^x mit $j \neq t$), der Wirkung von τ_a auf G_j^x (Beweis von 3.3.2), (i) und Anzahlgründen.

Wie wir 2.3.6 zu 2.3.7 verallgemeinert haben, läßt sich 3.4.14 für das TD über den nach 3.4.5 existierenden (t, r) -Differenzenmatrizen verallgemeinern. Sind dabei $w_1, \dots, w_n$ erzeugende Elemente von $GF(q_1)^*, \dots, GF(q_n)^*$, so setzen wir

$$\pi_{i_1, \dots, i_n} : (1, x_1, \dots, x_n) \mapsto (1, x_1 w_1^{i_1}, \dots, x_n w_n^{i_n})$$

und erhalten eine zu $\mathbb{Z}_{q_1-1} \oplus \dots \oplus \mathbb{Z}_{q_n-1}$ isomorphe Kollineationsgruppe $\mathfrak{M}$, für die zu 3.4.14 analoge Aussagen gelten. Die Einzelheiten seien dem Leser überlassen.

4. PROJEKTIVE TD-EBENEN

=====

In diesem Kapitel konstruieren wir projektive TD-Ebenen mit abelscher, auf den Punkten regulärer und auf den Geraden semiregulärer Kollineationsgruppe.

4.1 Grundlagen

Wir stellen zunächst wieder die benötigten Grundbegriffe zusammen. TD-Ebenen sind in einem bisher unveröffentlichten Manuskript von LENZ und JUNGnickel 1976 eingeführt worden. Alle in diesem Abschnitt zitierten Definitionen und Sätze sind aus diesem Manuskript übernommen. Wir verzichten auf die Übernahme von Beweisen sowie auf die größtmögliche Allgemeinheit.

4.1.1 Definition

Unter einer partiellen Ebene verstehen wir eine Inzidenzstruktur $\Delta = (\mathcal{P}, \mathcal{G}, I)$ mit folgenden Eigenschaften:

- (PE 1) $[p, q] \leq 1$ für je zwei verschiedene Punkte p und q .
- (PE 2) $[p] \geq 2$ für jeden Punkt p .
- (PE 3) $[G] \geq 3$ für jede Gerade G .
- (PE 4) Δ ist zusammenhängend, d.h. die von I erzeugte Äquivalenzrelation hat nur eine Klasse.

Gilt überdies noch

- (PE 5) $[p, q] \geq 1$ für je zwei verschiedene Punkte p und q .

heißt Δ ein PBD ('pairwise balanced design').

4.1.2 Definition

Δ und Δ' seien partielle Ebenen und $\delta: \Delta \rightarrow \Delta'$ ein Homomorphismus. δ heißt

stetig, falls das Urbild jedes Unterraumes ein Unter-
raum ist;

regulär, falls aus $p^{\delta} = q^{\delta}$ stets $[p, q] = 0$ oder $p = q$ folgt;

nichtdegeneriert, falls stets $\text{card } (G)^\delta \geq 2$ gilt;
abgeschlossen, falls das Bild jedes Unterraums ein
 Unterraum ist.

Dabei ist ein Unterraum einer Inzidenzstruktur eine
 Teilmenge der Punktmenge, die mit je zwei Punkten alle
 Punkte der (eventuellen) Verbindungsgeraden enthält.

4.1.3 Satz

Δ und Δ' seien partielle Ebenen und $\delta: \Delta \rightarrow \Delta'$ ein Homo-
 morphismus. Dann gilt:

- (i) δ ist genau dann regulär, wenn es stetig und
 nichtdegeneriert ist.
- (ii) δ ist genau dann abgeschlossen, wenn gilt:
 (4.1) Das Bild jeder Geraden ist ein Punkt oder
 eine Gerade.
 (4.2) $[p, q] = 0$ und $p^\delta \neq q^\delta$ implizieren stets
 $[p^\delta, q^\delta] = 0$.

4.1.4 Satz

Δ und Δ' seien endliche partielle Ebenen und δ ein regu-
 lärer, abgeschlossener Epimorphismus. G sei eine Gerade
 von Δ und $p_1', \dots, p_k'$ seien sämtliche mit G^δ inzidenten
 Punkte von Δ' . $p_1, \dots, p_k$ seien Urbilder von $p_1', \dots, p_k'$.
 Für jeden Punkt p von Δ sei mit N_p die Menge der Punkte
 q von Δ mit $p^\delta = q^\delta$ bezeichnet (für Geraden sei N_G dual
 erklärt). Dann bilden die Geraden aus N_G zusammen mit den
 Punkten aus den Punktklassen $N_{p_1}, \dots, N_{p_k}$ ein (t, k) -TD;
 dabei hängt t nicht von der Wahl von G ab.

4.1.5 Definition

Unter den Voraussetzungen von 4.1.4 setzen wir

$$(4.3) \quad r+1 := \max \{ [G'] : G' \in \Delta' \}$$

und nennen das Tripel $(\Delta, \Delta', \delta)$ eine (t, r) -TD-Ebene.

4.1.6 Satz

Eine (t, r) -TD-Ebene (Π, Π', ω) existiert bei gegebener Bildebene Π' mit Parameter r gemäß (4.1) genau dann, wenn ein $(t, r+1)$ -TD existiert.

4.2 PTD-Ebenen

In diesem Abschnitt wollen wir eine mehr inzidenzgeometrische Darstellung von TD-Ebenen entwickeln, besonders im Falle von projektiven Bildebenen.

4.2.1 Definition

$\Pi = (\mathfrak{P}, \mathfrak{B}, I)$ sei eine partielle Ebene mit

(TDE 1) Die durch

$$(4.4) \quad p \circ q \Leftrightarrow p=q \vee [p, q]=0$$

auf $\mathfrak{P}$ definierte Relation ist eine Äquivalenzrelation.

(TDE 2) Aus $pIG, H; qIG; rIH; q\phi p\phi r$ und qor folgt stets GoH . (Hierbei ist die von $\circ$ auf $\mathfrak{B}$ erzeugte Äquivalenzrelation wieder mit $\circ$ bezeichnet worden, vgl. 2.2.5).

(TDE 3) Es gibt drei Punkte p, q, r in allgemeiner Lage, d.h. es gilt $p\phi q\phi r\phi p$ und $pq \phi pr \phi qr \phi pq$.

Dann heißt Π eine PBTD-Ebene.

Axiom (TDE 1) sagt lediglich aus, daß Π ein GDD ('group divisible design') ist. Der Grund für die Wahl des Namens PBTD-Ebene wird sich aus 4.2.3 ergeben.

4.2.2 Definition

$\Pi = (\mathfrak{P}, \mathfrak{B}, I)$ sei eine PBTD-Ebene. Wir definieren die Inzidenzstruktur $\Pi' := (\mathfrak{P}', \mathfrak{B}', I')$ mit $\mathfrak{P}' := \{p' : p \in \mathfrak{P}\}$ und $\mathfrak{B}' := \{G' : G \in \mathfrak{B}\}$ durch $p' := \{q : q \in \mathfrak{P} \text{ und } poq\}$, $G' := \{H : H \in \mathfrak{B} \text{ und } GoH\}$ und $p'I'G'$ genau dann, wenn es qoq und HoG gibt mit qIH . Π' heißt die Bildebene von Π .

4.2.3 Satz

Π sei eine PBTD-Ebene. Dann ist Π' ein PBD und das Tripel (Π, Π', φ) , wo φ den natürlichen Epimorphismus von Π auf Π' bezeichnet, eine TD-Ebene im Sinne von 4.1.5.

Beweis:

Π' erfüllt offensichtlich (PE 3) und (PE 4), da Π dies tut und da (TDE 1) gilt. Seien nun Punkte p', q' mit $p' \neq q'$ gegeben. Es seien p, q Urbilder von p', q' . Wegen $p \neq q$ gibt es nach (TDE 1) eine Gerade G mit $p, q \in G$, also $p', q' \in G'$. Π' erfüllt somit (PE 5). Angenommen, es gilt auch $p', q' \in H'$. Nach 4.2.2 gibt es Punkte p_1, q_1 und Geraden H_1, H_2 mit $p_1 \in p, q_1 \in q, H_1, H_2 \in H'$ und $q_1 \in H_1, p_1 \in H_2$. Nach 2.2.5 können wir o.B.d.A. $H_1 = H_2 =: H$ annehmen. Nach (TDE 1) ist die Gerade $K := pq_1$ wohldefiniert. Nach (TDE 2) folgt $G \cap K \cap H$, also $G' = H'$. Daher erfüllt Π' auch (PE 1).

Es bleibt die Gültigkeit von (PE 2) nachzuweisen. Sei also p' ein beliebiger Punkt von Π' und p ein Urbild. Nach (TDE 3) gibt es Punkte q, r, s in allgemeiner Lage. Falls $p \in \{q, r, s\}$, gilt offenbar $[p'] \geq 2$. Falls p zu einem der Punkte q, r, s in der Relation $\circ$ steht, etwa pos , folgt $pq \cap sq \cap sr \cap pr$ (nach (TDE 2)) und wieder $[p'] \geq 2$. Falls schließlich $p \not\in \{q, r, s\}$, betrachte man die Geraden pq und pr . Falls $pq \not\cap pr$ gilt, sind wir fertig; anderenfalls gilt $pq \cap pr$, denn sonst würde pq nach 2.2.5 Punkte $r_1 \in pr$ und $s_1 \in os$ enthalten und q', r', s' wären kollinear im Widerspruch zu (TDE 3). Daher gilt in jedem Fall $[p'] \geq 2$ und Π ist somit ein PBD.

Wir müssen noch nachweisen, daß φ regulär und abgeschlossen ist. Nach (TDE 1) gilt $[p, q] = 0$, falls $p^\varphi = q^\varphi$; also ist φ regulär. Nach 4.1.3.(ii) ist φ auch abgeschlossen: (4.1) ist nach 4.2.2 und 2.2.5 erfüllt und (4.2) nach (TDE 1). Folglich ist (Π, Π', φ) eine TD-Ebene.

4.2.4 Satz

Es sei (Π, Π', φ) eine TD-Ebene und Π' ein PBD. Dann ist Π eine PBTD-Ebene.

Beweis:

Wir setzen

$$(4.5) \quad p \circ q \Leftrightarrow p^\varphi = q^\varphi.$$

Offenbar ist $\circ$ eine Äquivalenzrelation. Wir müssen zeigen, daß $\circ$ mit der nach (4.4) definierten Relation übereinstimmt. Es sei $p \circ q$, $p \neq q$; dann gilt wegen der Regularität von φ $[p, q] = 0$. Ist andererseits $p \neq q$, so folgt, da Π' ein PBD ist, $[p^\varphi, q^\varphi] = 1$ und daher nach (4.2) aus der Abgeschlossenheit von φ auch $[p, q] = 1$. Π erfüllt somit (TDE 1).

Es mögen nun p, q, r, G, H die Voraussetzungen von (TDE 2) erfüllen. Dann gilt $p^\varphi, q^\varphi \in G^\varphi, H^\varphi$ (man beachte $q^\varphi = r^\varphi$), also nach (PE 1) $G^\varphi = H^\varphi$. Sei nun $s \in G$ beliebig. Wir müssen zeigen, daß es ein $t \in H$ gibt mit $s^\varphi = t^\varphi$. Dies folgt aus der Abgeschlossenheit von φ ; denn wegen (4.1) wirkt φ auf jeder Geraden surjektiv, da es aufgrund der Regularität nach 4.1.3.(i) nichtdegeneriert ist. Mit analogen Argumenten folgt die Existenz eines Punktes $y \in G$ mit $y \circ x$ für gegebenes $x \in H$. Nach 2.2.5 gilt somit $G \circ H$; Π erfüllt also (TDE 2).

Die Gültigkeit von (TDE 3) ist trivial, da Π' ein Dreieck enthält.

Somit ist Π wie behauptet eine PBTD-Ebene.

4.2.5 Korollar

Π sei eine PBTD-Ebene und $G \circ H \not\subseteq K$. Dann gilt $[G, K] = 0$ oder $[H, K] = 0$ oder G, H, K haben einen Punkt gemein.

Beweis:

Sei nämlich $p \in G, K$ und $q \in H, K$. Es folgt $p' = G' \cap K' = H' \cap K' = q'$, d.h. $p \circ q$ und daher nach (TDE 1) $p = q$.

4.2.6 Definition

Π sei eine PBTD-Ebene, die außerdem noch

(TDE 4) Für je zwei Geraden G, H gibt es Punkte p, q mit poq, pIG und qIH

erfüllt. Dann heißt Π eine projektive TD-Ebene (kurz: PTD-Ebene).

4.2.7 Lemma

Π sei eine PBTD-Ebene. Es seien p, G gegeben mit $p'IG'$. Dann gibt es eine Gerade H mit pIH oder G und einen Punkt q mit $p \circ qIG$.

Beweis:

Die zweite Behauptung gilt nach 2.2.5. Für den Nachweis des ersten Teiles wähle man einen Punkt r mit $p' \neq r'IG'$. Man setze $H := pr$. Es folgt $H' = p'r' = q'r' = G'$, also GoH .

4.2.8 Satz

Es sei Π eine PBTD-Ebene. Π ist genau dann eine PTD-Ebene, wenn Π' eine projektive Ebene ist.

Beweis:

' $\Rightarrow$ '

Π sei PTD-Ebene. G', H' seien beliebige Geraden von Π' mit $G' \neq H'$. G, H seien Urbilder von G', H' . Nach (TDE 4) gibt es Punkte pIG und qIH mit poq . es folgt $p'IG', H'$. Da Π' nach 4.2.3 ein PBD ist und nach (TDE 3) ein Dreieck und somit auch ein Viereck enthält (es seien p, q, r in allgemeiner Lage und $G := pq, H := pr$; nach (PE 3) gibt es auf G bzw. H je einen weiteren Punkt s bzw. t ; nach (TDE 1) bilden dann q', r', s', t' ein Viereck), ist Π' eine projektive Ebene.

' $\Leftarrow$ '

Π' sei eine projektive Ebene. Dann schneiden sich je zwei verschiedene Geraden G', H' von Π' , etwa in p' . Die Behauptung folgt nach 4.2.7.

4.2.9 Korollar

Wir bezeichnen mit $\mathfrak{E}_t$ das Spektrum aller Paare (t, r) , für die eine (t, r) -PTD-Ebene existiert. Dann gilt:

$$(t, r) \in \mathfrak{E}_t \Leftrightarrow (1, r) \in \mathfrak{E}_t \wedge N(t) \geq r-1.$$

Beweis:

Das folgt unmittelbar aus 4.2.8, 4.2.3, 4.2.4, 4.1.6 und 3.1.5.

4.2.10 Korollar

Π sei eine (t, r) -PTD-Ebene. Dann gilt:

- (i) r ist die Ordnung von Π' .
- (ii) Für jede Fahne (p, G) gibt es genau t Geraden H mit $p \in H \subset G$.
- (iii) $\text{card } p' = t$ für jeden Punkt p .
- (iv) $\text{card } G' = t^2$ für jede Gerade G .
- (v) $[p] = r+1$ für jeden Punkt p .
- (vi) $[G] = t(r+1)$ für jede Gerade G .
- (vii) Es gibt $t(r^2+r+1)$ Punkte.
- (viii) Es gibt $t^2(r^2+r+1)$ Geraden.
- (ix) Falls $t \neq 1$ gilt, folgt $r \leq t$.

Beweis:

Das folgt unmittelbar aus 4.2.8 und 4.1.4 unter Berücksichtigung von (4.1) sowie bekannten Eigenschaften projektiver Ebenen und TD's.

4.3 Reguläre PTD-Ebenen

4.3.1 Hilfssatz

$\pi: \Pi_1 \rightarrow \Pi_2$ sei ein bijektiver Homomorphismus von PBTD-Ebenen. Dann ist π sogar ein Isomorphismus und sowohl π als auch π^{-1} erhalten die Relation $\circ$.

Beweis:

Es sei $p'' \in G''$. Wir wählen einen Punkt $q \in G$ mit $q \neq p$. Dann ist $p'' \neq q''$, da π injektiv ist; ferner gilt $p'', q'' \in G''$ nach Voraussetzung bzw. weil π ein Homomorphismus ist. Nach (TDE 1) existiert $H := pq$, daher folgt $p'', q'' \in H''$. Da Π' eine partielle Ebene ist, gilt $H'' = G''$ und somit, weil π bijektiv ist, $H=G$. Also ist $p \in G$.

Ferner gilt xoy genau dann, wenn $[x,y]=0$ oder $x=y$, was mit $[x'',y'']=0$ oder $x''=y''$, d.h. $p'' \circ q''$ gleichbedeutend ist. Die Behauptung für Geraden folgt dann aus 2.2.5.

4.3.2 Korollar

π induziert einen Isomorphismus $\pi': \Pi_1' \rightarrow \Pi_2'$ durch

$$(p')^{\pi'} := (p'')' \quad \text{bzw.} \quad (g')^{\pi'} := (g'')'.$$

4.3.3 Definition

Eine PTD-Ebene Π heißt regulär, wenn sie eine abelsche Kollineationsgruppe $\mathcal{G}$ mit $\mathcal{G} = \mathcal{g} \oplus \mathcal{H}$ zuläßt, so daß gilt:

(4.6) $\mathcal{G}$ ist auf den Punkten von Π regulär und auf den Geraden von Π semiregulär.

(4.7) $\mathcal{H}$ bildet jede Punktklasse von Π regulär und jede Geradenklasse von Π semiregulär auf sich ab.

$\mathcal{g}$ ist dann offenbar auf den Punkten und Geraden von Π' regulär.

4.3.4 Definition

t und $r \geq 2$ seien natürliche Zahlen und $v := r^2 + r + 1$. $\mathcal{g}$ sei eine abelsche Gruppe der Ordnung v und $\mathcal{H}$ eine abelsche Gruppe der Ordnung t . Wir setzen $\mathcal{G} := \mathcal{g} \oplus \mathcal{H}$. Eine (t,r) -Differenzenfamilie über $\mathcal{G}$ ist eine Familie

$$\mathcal{D} = \{D_1, \dots, D_t\} \quad \text{von Teilmengen}$$

$$D_i = \{(a_0, d_{0i}), (a_1, d_{1i}), \dots, (a_r, d_{ri})\} \quad (i=0, \dots, t)$$

von $\mathcal{G}$, so daß die $tr(r+1)$ Differenzen

$(a_h, d_{hi}) - (a_k, d_{ki}) \quad (i=1, \dots, t; \quad h, k = 0, \dots, r; h \neq k)$
 jedes $(x, y) \in \mathcal{G}$ mit $x \neq 0$ enthalten (aus Anzahlgründen genau einmal).

$D := \{a_0, \dots, a_r\}$ ist dann offenbar eine gewöhnliche Differenzenmenge in $\mathcal{G}$. In allen bekannten Fällen ist dann $\mathcal{G} = \mathbb{Z}_V$.

4.3.5 Beispiele

- (i) $t=3, r=2, \mathcal{G} = \mathbb{Z}_7 \oplus \mathbb{Z}_3$:
 $D_1 := \{(1,1), (2,2), (4,0)\}; \quad D_2 := \{(1,2), (2,1), (4,0)\};$
 $D_3 := \{(1,0), (2,0), (4,0)\}$
- (ii) $t=4, r=3, \mathcal{G} = \mathbb{Z}_{13} \oplus \text{EA}(4)$:
 $D_1 := \{(0,1), (1,w), (3,w^2), (9,0)\};$
 $D_2 := \{(0,w), (1,w^2), (3,1), (9,0)\};$
 $D_3 := \{(0,w^2), (1,1), (3,w), (9,0)\};$
 $D_4 := \{(0,0), (1,0), (3,0), (9,0)\}.$

Dabei sei w erzeugendes Element von $\text{GF}(4)^*$.

4.3.6 Satz

Es sei $\mathcal{D}$ eine (t,r) -Differenzenfamilie über $\mathcal{G} = \mathcal{G} \oplus \mathcal{R}$. Wir definieren die Inzidenzstruktur $\Pi(\mathcal{D}) := (\mathcal{G}, \mathcal{B}(\mathcal{D}), \epsilon)$ durch

$$\mathcal{B}(\mathcal{D}) := \{D_i + x : i=0, \dots, t-1 \text{ und } x \in \mathcal{G}\}.$$

Dann ist $\Pi(\mathcal{D})$ eine bezüglich $\mathcal{G}$ reguläre (t,r) -PTD-Ebene.

Umgekehrt läßt sich jede bezüglich $\mathcal{G}$ reguläre (t,r) -PTD-Ebene so beschreiben.

Beweis:

' $\Rightarrow$ '

Es sei $\mathcal{D}$ eine (t,r) -Differenzenfamilie und $\Pi := \Pi(\mathcal{D})$ wie in der Behauptung definiert. Da mit $h \neq k$ nach 4.3.4 stets $a_h \neq a_k$ gilt, sind Punkte der Form (x, y) und (x, y') offenbar stets unverbindbar. Wir setzen also

$$(4.8) \quad (x, y) \circ (x', y') \iff x = x'$$

und betrachten Punkte $(x, y), (x', y')$ mit $x \neq x'$. Dann gibt es

Indizes i, h, k mit $(x-x', y-y') = (a_h, d_{hi}) - (a_k, d_{ki})$. Es folgt $(x, y), (x', y') \in D_i + (x-a_h, y-d_{hi})$. Ist umgekehrt $(x, y), (x', y') \in D_j + (u, v)$, so gibt es Indizes j, m, l mit $(x, y) = (a_l, d_{lj}) + (u, v)$ und $(x', y') = (a_m, d_{mj}) + (u, v)$. Also gilt $x-a_l = x'-a_m$ und $y-d_{lj} = y'-d_{mj}$, d.h. $(x-x', y-y') = (a_l, d_{lj}) - (a_m, d_{mj})$. Nach 4.3.4 folgt wegen der Eindeutigkeit der Differenzendarstellung $l=h, i=j, k=m$. Also erfüllt Π (PE 1) und (TDE 1). (PE 2), (PE 3) und (PE 4) sind trivialerweise erfüllt.

Offenbar erfüllt Π auch (TDE 3) (z.B. sind die Punkte $(a_0, d_{01}), (a_1, d_{11})$ und (x, y) mit $x \neq a_i$ für $i=0, \dots, r$ in allgemeiner Lage).

Es mögen nun p, q, r, G, H die Voraussetzungen von (TDE 2) erfüllen; es sei etwa $p = (x, y)$, $q = (x', y')$ und $r = (x'', y'')$. Es gelte etwa $(x, y) - (x', y') = (a_h, d_{hi}) - (a_k, d_{ki})$ und $(x, y) - (x'', y'') = (a_h, d_{hj}) - (a_k, d_{kj})$. Dann gilt

$$G = D_i + (x-a_h, y-d_{hi}) \quad \text{und} \quad H = D_j + (x-a_h, y-d_{hj}).$$

Nach 2.2.5 und (4.8) folgt offenbar GoH. Daher erfüllt Π auch (TDE 2), ist also eine PBTD-Ebene.

Da D eine Differenzenmenge in $\mathcal{G}$ ist, ist Π' offenbar eine projektive Ebene. Somit ist Π nach 4.2.8 eine PTD-Ebene.

Offenbar bilden die Abbildungen $\tau_{ab}: (x, y) \mapsto (x+a, y+b)$ eine zu $\mathcal{G}$ isomorphe Kollineationsgruppe von Π ; also ist Π klarerweise bezüglich $\mathcal{G}$ regulär und hat die Parameter (t, r) .

' $\Leftarrow$ '

Sei nun Π eine bezüglich $\mathcal{G}$ reguläre (t, r) -PTD-Ebene. Wir wählen willkürlich einen Basispunkt $p =: (0, 0)$. Der Punkt q , der sich durch Anwendung von $(x, y) \in \mathcal{G}$ auf p ergibt, erhält die Koordinaten (x, y) . Da $\mathcal{G}$ auf den Punkten regulär ist, entsprechen sich so Punkte und Koordinaten umkehrbar eindeutig. Da $\mathcal{G}$ auf den Geraden semiregulär ist, zerfällt die Geradenmenge nach 4.2.10 in t Orbits, auf

$\mathfrak{G}$ regulär ist. Wir wählen in jedem dieser Orbits willkürlich eine Basisgerade D_i und fassen sie als Punktmenge auf, etwa

$$D_i = \{(a_0, d_{0i}), (a_1, d_{1i}), \dots, (a_r, d_{ri})\} \quad (i=1, \dots, t).$$

Sei nun $(x, y) \in \mathfrak{G}$ mit $x \neq 0$ beliebig gegeben. Nach (TDE 1) sind die Punkte $(0, 0)$ und (x, y) eindeutig verbindbar, etwa durch $D_i + (u, v)$. Es sei etwa

$$(x, y) = (a_h, d_{hi}) + (u, v) \quad \text{und} \quad (0, 0) = (a_k, d_{ki}) + (u, v).$$

Dann folgt $(x, y) = (a_h, d_{hi}) - (a_k, d_{ki})$. Daher ist

$\mathfrak{D} := \{D_1, \dots, D_t\}$ eine (t, r) -Differenzenfamilie über $\mathfrak{G}$. Offenbar gilt $\Pi \approx \Pi(\mathfrak{D})$.

4.3.7 Satz

$\mathfrak{D}$ sei eine (t, r) -Differenzenfamilie über $\mathfrak{G}$, wie in 4.3.4 beschrieben. Dann ist die $(r+1) \times t$ -Matrix $D = (d_{ij})$ eine $(t, r, \mathfrak{N})$ -Differenzenmatrix.

Sei umgekehrt $D = (d_{ij})$ eine $(t, r, \mathfrak{N})$ -Differenzenmatrix und $\{a_0, \dots, a_r\}$ eine Differenzenmenge in $\mathfrak{g}$. Dann ist das nach 4.3.4 gebildete $\mathfrak{D}$ eine (t, r) -Differenzenfamilie über $\mathfrak{G}$.

Beweis:

' $\Rightarrow$ '

$\mathfrak{D}$ sei eine (t, r) -Differenzenfamilie. Es seien $i, j \in \{0, \dots, r\}$ mit $i \neq j$ gegeben. Nach 4.3.4 sind alle Differenzen

$$(a_i, d_{ik}) - (a_j, d_{jk}) \quad (k=0, \dots, t)$$

verschieden, also müssen alle Elemente $d_{ik} - d_{jk}$ ($k=0, \dots, t$) verschieden sein. Somit ist D eine $(t, r, \mathfrak{N})$ -Differenzenmatrix.

' $\Leftarrow$ '

Sei nun $D = (d_{ik})$ ($i=0, \dots, r$; $k=0, \dots, t$) eine $(t, r, \mathfrak{N})$ -Differenzenmatrix und $\{a_0, \dots, a_r\}$ eine Differenzenmenge in $\mathfrak{g}$. Wir betrachten Differenzen $(a_i, d_{ik}) - (a_j, d_{jk})$ und $(a_i, d_{i, k'}) - (a_j, d_{j, k'})$. Falls beide Differenzen gleich

sind, folgt zunächst $i=i'$ und $j=j'$, da $\{a_0, \dots, a_r\}$ eine Differenzenmenge ist. Dann folgt aber auch $k'=k$, da D eine Differenzenmatrix ist. Aus Anzahlgründen muß also jedes Element $(x, y) \in \mathfrak{G}$ mit $x \neq 0$ unter den Differenzen $(a_i, d_{ik}) - (a_j, d_{jk})$ genau einmal auftreten. Somit ist $\mathfrak{D}$ eine (t, r) -Differenzenfamilie über $\mathfrak{G}$.

4.3.8 Korollar

t und r seien natürliche Zahlen mit $r \geq 2$. Dann ist $(t, r) \in \mathfrak{RP}$ (wo $\mathfrak{RP}$ das Spektrum aller (t, r) bezeichnet, für die eine reguläre (t, r) -PTD-Ebene existiert) genau dann, wenn $(1, r) \in \mathfrak{RP}$ gilt und eine (t, r) -Differenzenmatrix existiert.

Beweis:

Das folgt unmittelbar aus 4.3.7 und 4.3.6.

4.3.9 Korollar

Es ist $(t, r) \in \mathfrak{RP}$ in mindestens den folgenden Fällen:

- (i) t Primzahlpotenz, $r \leq t-1$.
- (ii) $t = q_1 \dots q_n$, q_i Primzahlpotenz und $r \leq q_i - 1$ für $i = 1, \dots, n$.
- (iii) $t = q^2 + q + 1$, q Primzahlpotenz, $N(q+1) \geq r$.
- (iv) $t = q^2 - 1$, q Primzahlpotenz und es gibt $(q-1, r, \mathbb{Z}_{q-1})$ -Differenzenmatrizen.

Beweis:

Das folgt unmittelbar aus 4.3.8 mit 3.3.1, 3.3.5, 3.3.10 und 3.3.12.

4.3.10 Korollar

Es sei $t \equiv 2 \pmod{4}$. Dann gilt $(t, r) \notin \mathfrak{RP}$ für jedes r .

Beweis:

Das folgt unmittelbar aus 4.3.8 mit 3.3.8.

4.3.11 Satz

t und r seien Primzahlpotenzen mit $2 \leq r < t$ und Π die gemäß 4.3.7 und 4.3.6 aus der in 3.4.1 beschriebenen $(t, r, EA(t))$ -Differenzenmatrix und einer nach dem Satz von SINGER 1938 existenten Differenzenmenge $\{a_0, \dots, a_r\}$ in $\mathbb{Z}_{r^2+r+1}^2$ konstruierte (t, r) -PTD-Ebene. $\mathcal{R}$ sei die Gruppe der im Beweis von 4.3.6 beschriebenen Kollineationen τ_{ab} . Dann bilden die Abbildungen $\pi_1: (x, y) \mapsto (x, yw^i)$ eine zu $\mathbb{Z}_{t-1}$ isomorphe Kollineationsgruppe $\mathcal{M}$ von Π . $\mathcal{U}$ sei die von $\mathcal{R}$ und $\mathcal{M}$ erzeugte Kollineationsgruppe. Dann gilt:

- (i) $\mathcal{U}$ ist das halbdirekte Produkt von $\mathcal{R}$ mit $\mathcal{M}$.
- (ii) $\mathcal{U}$ ist auf jeder Punktklasse scharf zweifach transitiv.
- (iii) Die Geradenmenge

$$\{D_1 + x: x \in \mathbb{Z}_{r^2+r+1} \oplus EA(t) \text{ und } i=1, \dots, t-1\}$$

ist ein Orbit, auf dem $\mathcal{U}$ treu operiert.

Beweis:

Völlig analog zum Beweis von Satz 3.3.14.

Benutzt man die Differenzenmatrix aus 3.4.5 statt der aus 3.4.1, so ist eine weitere Verallgemeinerung - entsprechend den Bemerkungen nach 3.4.14 - möglich. Dies sei dem Leser überlassen.

5. NORMALE EBENEN UND NTD-EBENEN

Abschließend beschäftigen wir uns mit 'normalen Ebenen', die einer Verallgemeinerung der gewöhnlichen Differenzfamilien entsprechen. PTD-Ebenen sind spezielle Beispiele. Wir erhalten u.a. neue Ergebnisse über die Existenz von Blockplänen mit regulärer abelscher Kollineationsgruppe. Schließlich konstruieren wir reguläre TD-Ebenen, deren Bildebenen normale Ebenen sind.

5.1 Normale Ebenen

5.1.1 Definition

Eine partielle Ebene Π heißt eine normale Ebene, wenn Π eine abelsche Kollineationsgruppe $\mathcal{G}$ zuläßt, so daß gilt:

(5.1) $\mathcal{G}$ ist auf den Punkten von Π regulär.

(5.2) $\mathcal{G}$ ist auf den Geraden von Π semiregulär.

(5.3) $[H]$ ist unabhängig von der Wahl der Geraden H .

5.1.2 Hilfssatz

Eine normale Ebene Π ist eine taktische Konfiguration. Für die Parameter v (= Anzahl der Punkte von Π), b (= Anzahl der Geraden von Π), k ($= [G]$ für jede Gerade G) und r ($= [p]$ für jeden Punkt p) gilt außer der bekannten Beziehung

$$(5.4) \quad vr = bk$$

noch

$$(5.5) \quad k \mid r.$$

Beweis:

Seien p, q beliebige Punkte von Π . Nach Voraussetzung gibt es eine Kollineation σ mit $p^\sigma = q$. Da σ eine inzidenzerhaltende Bijektion ist, folgt $[p] = [q] =: r$.

Da $\mathcal{G}$ regulär auf den Punkten von Π ist, folgt $o(\mathcal{G}) = v$. Da $\mathcal{G}$ semiregulär auf den Geraden von Π ist, folgt $v \mid b$, woraus sich mit (5.4) sofort (5.5) ergibt.

5.1.3 Definition

Mit den Bezeichnungen aus 5.1.2 setzen wir $s := \frac{r}{k}$ und nennen Π eine (bzgl. $\mathcal{G}$ normale) (v, k, s) -Ebene.

Dann sind z.B. die desarguesschen projektiven Ebenen $(q^2+q+1, q+1, 1)$ -Ebenen und reguläre (t, k) -PTD-Ebenen $(t(k^2+k+1), k+1, t)$ -Ebenen. Für weitere Beispiele vgl. man 5.1.5 und 5.1.7.

5.1.4 Definition

$\mathcal{G}$ sei eine abelsche Gruppe der Ordnung v . Eine (v, k, s) -Differenzenfamilie in $\mathcal{G}$ ist eine Menge $\mathcal{D} = \{D_1, \dots, D_s\}$ von Teilmengen $D_i = \{d_{i1}, \dots, d_{ik}\}$ von $\mathcal{G}$ mit $k \geq 3$, so daß gilt:

(5.6) Die Differenzen

$$d_{ij} - d_{i1} \quad (i=1, \dots, s; j, l = 1, \dots, k; j \neq l)$$

sind paarweise verschieden.

und

$$(5.7) \quad \Delta := \{d_{ij} - d_{i1} : i=1, \dots, s; j, l = 1, \dots, k; j \neq l\}$$

ist ein Erzeugendensystem von $\mathcal{G}$.

Gilt statt (5.7) sogar

$$(5.8) \quad \Delta = \mathcal{G} \setminus \{0\},$$

heißt $\mathcal{D}$ eine maximale (v, k) -Differenzenfamilie. Offenbar ist $\mathcal{D}$ genau dann maximal, wenn gilt $s = \frac{v-1}{k(k-1)}$.

In dieser Terminologie ist eine (t, r) -Differenzenfamilie - wie in 4.3.4 definiert - eine $(t(r^2+r+1), r+1, t)$ -Differenzenfamilie. Wir bemerken, daß maximale Differenzenfamilien in der Literatur gewöhnlich als 'einfache Differenzenfamilien' bezeichnet werden.

5.1.5 Satz

$\mathcal{D}$ sei eine (v, k, s) -Differenzenfamilie in $\mathcal{G}$. Wir definieren die Inzidenzstruktur $\Pi(\mathcal{D}) := (\mathcal{G}, \mathcal{B}(\mathcal{D}), \epsilon)$ durch

$\mathfrak{B}(\mathfrak{D}) := \{D_i + x: i=1, \dots, s \text{ und } x \in \mathfrak{G}\}$. Dann ist $\Pi(\mathfrak{D})$ eine bzgl. $\mathfrak{G}$ normale (v, k, s) -Ebene. Ist $\mathfrak{D}$ maximal, so ist $\Pi(\mathfrak{D})$ ein Blockplan.

Umgekehrt ist jede bzgl. $\mathfrak{G}$ normale (v, k, s) -Ebene so darstellbar. Dabei führt ein Blockplan auf eine maximale Differenzenfamilie.

Beweis:

' $\Rightarrow$ '

Es sei $\mathfrak{D}$ eine (v, k, s) -Differenzenfamilie und $\Pi := \Pi(\mathfrak{D})$ wie in der Behauptung definiert. Die Bedingungen (5.1), (5.2) und (5.3) sind offensichtlich erfüllt. Es bleibt zu zeigen, daß Π eine partielle Ebene ist (vgl. 4.1.1). (PE 2) und (PE 3) sind offenbar erfüllt. Angenommen, die Punkte x und y wären auf mindestens zwei Geraden, etwa $D_i + u$ und $D_j + v$. Dann folgt:

$$x = d_{ih} + u = d_{jl} + v \quad \text{und} \quad y = d_{im} + u = d_{jn} + v$$

für geeignete Indizes h, l, m, n . Dann wäre aber

$$x - y = d_{ih} - d_{im} = d_{jl} - d_{jn}$$

im Widerspruch zu (5.6). Daher erfüllt Π auch (PE 1).

Es bleibt noch (PE 4) zu bestätigen. Dazu genügt es zu zeigen, daß zu je zwei Punkten x, y eine Punktfolge $x = x_0, x_1, \dots, x_{n-1}, x_n = y$ existiert mit $[x_i, x_{i-1}] = 1$ für $i=1, \dots, n$.

Nach (5.7) gibt es eine Darstellung

$$(5.9) \quad x - y = (d_{i_1 j_1} - d_{i_1 l_1}) + \dots + (d_{i_n j_n} - d_{i_n l_n}).$$

Wir setzen

$$(5.10) \quad x_0 := x; \quad x_h := d_{i_h l_h} + x_{h-1} - d_{i_h j_h}$$

für $h=1, \dots, n$.

Dann folgt

$$x_{h-1} = d_{i_h j_h} + x_{h-1} - d_{i_h j_h} \in D_{i_h} + (x_{h-1} - d_{i_h j_h})$$

und wegen (5.10)

$$x_h = d_{i_h l_h} + x_{h-1} - d_{i_h j_h} \in D_{i_h} + (x_{h-1} - d_{i_h j_h})$$

für $h=1, \dots, n$. Somit gilt $[x_h, x_{h-1}] = 1$ für $h=1, \dots, n$ und offenbar ist wegen (5.9) und (5.10) $x_n = y$. Also gilt auch (PE 4), d.h. Π ist normale (v, k, s) -Ebene.

Sei nun $\mathfrak{D}$ sogar maximal. Sind x, y mit $x \neq y$ beliebig gegeben, so gibt es eine Darstellung $y - x = d_{ij} - d_{i_1 j_1}$. Die soeben mit (5.9) und (5.10) durchgeführte Argumentation liefert dann (mit $n=1$) direkt $[x, y] = 1$. Also ist Π ein Blockplan, da es nach 5.1.2 taktische Konfiguration ist.

' $\Leftarrow$ '

Sei nun Π eine beliebige bzgl. $\mathfrak{G}$ normale (v, k, s) -Ebene. Wir wählen willkürlich einen Basispunkt $p =: 0$. Der Punkt q , der durch Anwendung von $x \in \mathfrak{G}$ aus p hervorgeht, erhält die Koordinate x . In jedem Geradenorbit (nach Definition gibt es s derartige Orbits) wählen wir eine Basisgerade, etwa $D_i = \{d_{i1}, \dots, d_{ik}\}$ ($i=1, \dots, s$); k hängt nach 5.1.2 nicht von der Wahl der Geraden ab und ist nach (PE 3) ≥ 3 . Jede Gerade ist dann eindeutig in der Form $D_i + x$ darstellbar.

Wir setzen $\mathfrak{D} := \{D_1, \dots, D_s\}$.

$\mathfrak{D}$ erfüllt (5.6); wäre nämlich etwa $x = d_{i_h} - d_{i_m} = d_{j_l} - d_{j_n}$, so wären sowohl $D_i + (x - d_{i_h})$ als auch $D_j + (x - d_{j_l})$ Verbindungsgeraden von 0 und x , im Widerspruch zu (PE 1). Es bleibt die Gültigkeit von (5.7) nachzuprüfen. Sei $x \neq 0$ beliebig. Wegen (PE 4) gibt es Punkte $0 = x_0, x_1, \dots, x_{n-1}, x_n = x$ mit $[x_h, x_{h-1}] = 1$ für $h=1, \dots, n$, etwa $x_h, x_{h-1} \in D_{i_h} + u_h$.

Dann folgt

$$x_h = d_{i_h l_h} + u_h \quad \text{und} \quad x_{h-1} = d_{i_h j_h} + u_h \quad (h=1, \dots, n)$$

für geeignete j_h, l_h und somit

$$(5.11) \quad x_h = d_{i_h l_h} + x_{h-1} - d_{i_h j_h} \quad (h=1, \dots, n),$$

$$x_n = x \quad \text{und} \quad x_0 = 0.$$

Aus (5.11) ergibt sich nun direkt

$$x = (d_{i_n l_n} - d_{i_n j_n}) + \dots + (d_{i_1 l_1} - d_{i_1 j_1}).$$

Also ist auch (5.7) erfüllt und $\mathfrak{D}$ somit eine (v,k,s) -Differenzenfamilie.

Sei schließlich Π ein Blockplan. Dann kann man in der eben mit (5.11) durchgeführten Argumentation $n=1$ setzen und erhält direkt für $x \neq 0$ eine Darstellung $x = d_{i1} - d_{ij}$; also ist $\mathfrak{D}$ dann maximal.

Daß $\Pi \approx \Pi(\mathfrak{D})$ gilt, ist offensichtlich.

5.1.6 Definition

Wir bezeichnen mit $\mathfrak{ES}$ das Spektrum der Tripel (v,k,s) , für die eine normale (v,k,s) -Ebene existiert, mit $\mathfrak{EK}$ das Spektrum der (v,k) , für die ein normaler (v,k) -Blockplan existiert und mit $\mathfrak{ED}$ das Spektrum der (t,r) , für die eine (t,r) -Differenzenmatrix existiert.

5.1.7 Hilfssatz

Es gilt $(v,k,s) \in \mathfrak{ES}$ in mindestens den folgenden Fällen:

- (i) q Primzahlpotenz, $v=q^2+q+1$, $k=q+1$, $s=1$
- (ii) q Primzahlpotenz, $v=q^2-1$, $k=q$, $s=1$
- (iii) $(t,r) \in \mathfrak{ED}$, r Primzahlpotenz, $v=t(r^2+r+1)$,
 $k=r+1$, $s=t$.
- (iv) v Primzahlpotenz mit $v=k(k-1)s+1$ und $e^{k^2} k^{2k} < v$.
- (v) $v = 6s+1$ Primzahlpotenz, $k=3$.
- (vi) $v \geq 2^k - 1$, $s=1$.

Für die Paare (v,k) nach (i),(iv),(v) gilt sogar $(v,k) \in \mathfrak{EK}$.

Beweis:

- (i) Nach dem Satz von SINGER 1938 gibt es zu jeder Primzahlpotenz q eine Differenzenmenge in $\mathbb{Z}_q^{2+q+1}$.
- (ii) Nach BOSE 1942 gibt es zu jeder Primzahlpotenz q eine affine Differenzenmenge in $\mathbb{Z}_q^{2-1}$ (s.a. HOFFMANN 1952 oder DEMBOWSKI 1968 p. 210-211).
- (iii) nach 4.3.8 und 4.2.10.
- (iv) nach WILSON 1974b Corollary 2.1 (über $GF(v)$).
- (v) nach BOSE 1939, p.374.

(vi) Wir benutzen die Gruppe $\mathbb{Z}_v$ und setzen

$D := \{0, 1, 3, \dots, 2^{k-1} - 1\}$. Man sieht sofort, daß die Differenzen $(2^m - 1) - (2^n - 1) = 2^m - 2^n$ für $n < m$ und $m, n = 0, \dots, k-1$ alle verschieden und (als Elemente von $\mathbb{Z}$ aufgefaßt) $\leq 2^{k-1} - 1$ sind; wegen $v \geq 2^{k-1}$ sind dann auch die Differenzen $(2^n - 1) - (2^m - 1)$ alle verschieden und von den oben betrachteten ebenfalls verschieden. Wegen $1 \in \Delta$ folgt auch $\langle \Delta \rangle = \mathbb{Z}_v$.

5.2 Kompositionsmethoden, NTD- und BDTD-Ebenen

5.2.1 Satz

k sei Primzahlpotenz. Falls es (v, k, s) - und (v', k, s') -Differenzenfamilien gibt, gibt es auch $(vv', k, k(k-1)ss' + s + s')$ -Differenzenfamilien.

Falls es maximale (v, k) - und (v', k) -Differenzenfamilien gibt, gibt es auch eine maximale (vv', k) -Differenzenfamilie.

Beweis:

Es sei $\mathfrak{D} = \{D_1, \dots, D_s\}$ mit $D_i = \{d_{i1}, d_{i2}, \dots, d_{ik}\}$ ($i=1, \dots, s$) eine (v, k, s) -Differenzenfamilie und $\mathfrak{D}' = \{D'_1, \dots, D'_{s'}\}$ mit $D'_j = \{d'_{j1}, \dots, d'_{jk}\}$ ($j=1, \dots, s'$) eine (v', k, s') -Differenzenfamilie über $\mathfrak{G}$ bzw. $\mathfrak{G}'$. Wir werden eine Differenzenfamilie mit den gewünschten Parametern über $\mathfrak{G} \oplus \mathfrak{G}'$ erklären.

Da k Primzahlpotenz ist, gibt es $k-1$ paarweise orthogonale lateinische Quadrate der Ordnung k , etwa $A_2, \dots, A_k$ (o.B.d.A. auf der Symbolmenge $\{1, \dots, k\}$ und sämtlich mit erster Zeile $1, \dots, k$). A_1 sei die $k \times k$ -Matrix mit allen Zeilen $1, \dots, k$. Wir bezeichnen mit $\vec{a}_j^i$ die j -te Zeile von A_i und setzen

$$B := \begin{pmatrix} \vec{a}_2^1 & \dots & \vec{a}_k^1 \\ \vdots & & \vdots \\ \vec{a}_2^k & \dots & \vec{a}_k^k \end{pmatrix} = \begin{pmatrix} b_{11} & \dots & b_{1, k(k-1)} \\ \vdots & & \vdots \\ b_{k1} & \dots & b_{k, k(k-1)} \end{pmatrix}$$

Dann ist B eine $k \times k(k-1)$ -Matrix, so daß für je zwei ver-

schiedene Zeilen i, j die Paare (b_{ix}, b_{jx}) jedes Paar (m, n) mit $m \neq n$ ($m, n = 1, \dots, k$) genau einmal enthalten.

Wir definieren nun eine Menge $\mathfrak{D}''$ wie folgt:

Für jedes $i=1, \dots, s$, jedes $j=1, \dots, s'$ und jedes $l=1, \dots, k(k-1)$ enthalte $\mathfrak{D}''$ die Menge

$$D_1^{ij} := \{(d_{i1}, d'_{j1_1}), \dots, (d_{ik}, d'_{jl_k})\}$$

mit $l_p := b_{\rho 1}$ für $\rho=1, \dots, k$ und $l=1, \dots, k(k-1)$.

Ferner enthalte $\mathfrak{D}''$ die Mengen

$$\bar{D}_i := \{(d_{i1}, 0), \dots, (d_{ik}, 0)\} \quad (i=1, \dots, s)$$

und

$$\bar{D}'_j := \{(0, d_{j1}), \dots, (0, d_{jk})\} \quad (j=1, \dots, s').$$

Wir behaupten, daß $\mathfrak{D}''$ eine $(vv', k, k(k-1)ss' + s + s')$ -Differenzenfamilie ist.

Aus den Mengen $\bar{D}_i$ ergeben sich offenbar nur Differenzen der Form $(x, 0)$, die sämtlich verschieden sind, weil $\mathfrak{D}$ eine Differenzenfamilie ist. Entsprechend ergeben sich aus den Mengen $\bar{D}'_j$ nur verschiedene Differenzen der Form $(0, y)$.

Es bleiben also die D_1^{ij} zu betrachten. Für jedes j und l sind die Elemente $d'_{j1_1}, \dots, d'_{jl_k}$ paarweise verschieden, da keine Spalte von B zweimal dasselbe Element enthalten kann. Alle Differenzen, die sich aus den D_1^{ij} ergeben, haben also die Form (x, y) mit $x, y \neq 0$, sind also von den schon betrachteten Differenzen verschieden. Falls etwa gilt

$$(x, y) = (d_{ia}, d'_{jl_a}) - (d_{ib}, d'_{jl_b}) = (d_{hc}, d'_{mn_c}) - (d_{hd}, d'_{mn_d}),$$

so folgt sofort $d_{ia} - d_{ib} = d_{hc} - d_{hd}$ und daher, weil $\mathfrak{D}$ Differenzenfamilie ist, $i=h$, $a=c$ und $b=d$. Damit ergibt sich weiter $d'_{jl_c} - d'_{jl_d} = d'_{mn_c} - d'_{mn_d}$ und da auch $\mathfrak{D}'$ Differenzenfamilie ist $j=m$, $l_c = n_c$ und $l_d = n_d$, d.h. $b_{cl} = b_{cn}$ und $b_{dl} = b_{dn}$.

Aus der oben erwähnten Orthogonalitätseigenschaft von B folgt also $l=n$. Die beiden Darstellungen von (x, y) sind also identisch, d.h. $\mathfrak{D}''$ erfüllt (5.6).

Da $\mathfrak{D}$ und $\mathfrak{D}'$ (5.7) erfüllen, ist das auch für $\mathfrak{D}''$ der Fall (bereits diejenigen Differenzen, die sich aus den $\overline{D}_i$ und $\overline{D}_j'$ ergeben, erzeugen $\mathfrak{G} \oplus \mathfrak{G}'$).

Daß $\mathfrak{D}''$ die angegebenen Parameter hat, ist offensichtlich.

Falls in dieser Konstruktion $\mathfrak{D}$ und $\mathfrak{D}'$ maximal waren, ist es auch $\mathfrak{D}''$; denn dann gilt

$$s = \frac{v-1}{k(k-1)} \quad \text{und} \quad s' = \frac{v'-1}{k(k-1)},$$

also

$$\begin{aligned} s'' &= \frac{v-1}{k(k-1)} \cdot \frac{v'-1}{k(k-1)} \cdot k(k-1) + \frac{(v-1)+(v'-1)}{k(k-1)} \\ &= \frac{vv'-1}{k(k-1)}; \end{aligned}$$

somit ist $\mathfrak{D}''$ offenbar maximal.

5.2.2 Korollar

q und $q+1$ seien Primzahlpotenzen. Dann gibt es normale Blockpläne mit Parametern $k=q+1$ und $v=(q^2+q+1)^n$ für jedes $n \in \mathbb{N}$.

Beweis:

Das folgt aus 5.2.1, 5.1.7.(i) und 5.1.5.

5.2.3 Beispiele

q	2	3	4	7	8	16	31	127
k	3	4	5	8	9	17	32	128
v	7^n	13^n	21^n	57^n	73^n	273^n	993^n	16257^n etc.

5.2.4 Korollar

k sei Primzahlpotenz. Dann gibt es normale Blockpläne mit Parametern k und v für jedes v , für das sämtliche Faktoren der Primzahlpotenzzzerlegung hinreichend groß (z.B. $> e^{k^2} k^{2k}$) und $\equiv 1 \pmod{k(k-1)}$ sind.

Beweis:

Das folgt aus 5.2.1, 5.1.7.(iv) und 5.1.5.

5.2.4 stellt eine gewisse Verbesserung der Resultate von Wilson dar: WILSON 1974b zeigte, daß es für hinreichend große Primzahlpotenzen v mit der notwendigen Bedingung $v \equiv 1 \pmod{k(k-1)}$ normale (v,k) -Blockpläne gibt; WILSON 1975 zeigte, daß es für jedes hinreichend große v mit der notwendigen Bedingung (v,k) -Blockpläne gibt. Allerdings konnte er dabei keine Aussagen über eventuelle Automorphismen machen. Unser Resultat ist zwar insofern schlechter, als es nicht für alle hinreichend großen v gilt, sondern nur für solche, für die sämtliche Faktoren der Primzahlpotenzzerlegung hinreichend groß sind und die notwendigen Bedingungen erfüllen, aber auch andererseits wesentlich stärker, da es für alle diese v eine auf den Punkten reguläre und den Geraden semireguläre abelsche Kollineationsgruppe liefert.

5.2.5 Definition

Eine NTD-Ebene ist eine TD-Ebene (siehe 4.1.5), deren Bildebene eine normale Ebene ist. Eine BDTD-Ebene ist eine TD-Ebene, deren Bildebene ein Blockplan ('block design') ist.

5.2.6 Definition

Eine TD-Ebene heißt regulär, wenn sie eine abelsche Kollineationsgruppe $\mathfrak{G} = \mathfrak{g} \oplus \mathfrak{n}$ zuläßt, so daß gilt:

(5.12) $\mathfrak{G}$ ist auf den Punkten regulär und auf den Geraden semiregulär.

(5.13) $\mathfrak{n}$ bildet jede Punktklasse regulär auf sich ab.

Offenbar ist dann die Bildebene eine bezüglich $\mathfrak{g}$ normale Ebene.

5.2.7 Satz

② sei eine (v,k,s) -Differenzenfamilie über $\mathfrak{g}$ und $A = (a_{i,j})$ ($i=1, \dots, k$; $j=1, \dots, t$) eine $(t,k-1)$ -Differenzenmatrix über $\mathfrak{n}$.

Wir setzen

$$D_{ij} := \{(d_{i1}, a_{1j}), \dots, (d_{ik}, a_{kj})\}$$

für $i=1, \dots, s$ und $j=1, \dots, t$. Dann ist $\mathfrak{D}' := \{D_{ij} : i=1, \dots, s \text{ und } j=1, \dots, t\}$ eine (vt, k, st) -Differenzenfamilie über $\mathfrak{G} := \mathfrak{g} \oplus \mathfrak{R}$. Die nach 5.1.5 aus $\mathfrak{D}'$ entstehende normale Ebene Π ist eine bzgl. $\mathfrak{G}$ reguläre $(t, k-1)$ -NTD-Ebene über der nach 5.1.5 aus $\mathfrak{D}$ entstehenden normalen (v, k, s) -Ebene Π' . Falls $\mathfrak{D}$ maximal ist, ist Π sogar BDTD-Ebene.

Umgekehrt läßt sich jede bezüglich $\mathfrak{G}$ normale $(t, k-1)$ -NTD-Ebene wie beschrieben darstellen.

Beweis:

' $\Rightarrow$ '

Angenommen, $(x, y) \in \mathfrak{G}$ besitzt zwei Differenzendarstellungen, etwa

$$(x, y) = (d_{il}, a_{lj}) - (d_{im}, a_{mj}) = (d_{hn}, a_{nb}) - (d_{hc}, a_{cb}).$$

Dann folgt zunächst $d_{il} - d_{im} = d_{hn} - d_{hc}$ und somit, da $\mathfrak{D}$ eine Differenzenfamilie ist, $i=h$, $l=n$ und $m=c$. Daraus folgt weiter $a_{lj} - a_{mj} = a_{lb} - a_{mb}$ und somit, da A eine Differenzenmatrix ist, $b=j$. Also sind die beiden Darstellungen identisch und $\mathfrak{D}'$ erfüllt (5.6).

Ist $x \in \mathfrak{g}$ als Differenz aus $\mathfrak{D}$ darstellbar, etwa $x = d_{il} - d_{im}$, so ist in $\mathfrak{D}'$ jedes Element der Form (x, y) darstellbar: Da A Differenzenmatrix ist, gibt es nämlich einen Index j mit $a_{lj} - a_{mj} = y$. Dann gilt aber $(x, y) = (d_{il}, a_{lj}) - (d_{im}, a_{mj})$. Somit ist offenbar die Menge Δ' der sich aus $\mathfrak{D}'$ ergebenden Differenzen ein Erzeugendensystem für $\mathfrak{G}$, da Δ ein Erzeugendensystem für $\mathfrak{g}$ ist. Also erfüllt $\mathfrak{D}'$ auch (5.7) und ist somit eine Differenzenfamilie, die offenbar die angegebenen Parameter besitzt.

Wir setzen nun

$$(5.14) \quad (x, y) \circ (x', y') :\Leftrightarrow x=x'$$

für Punkte $(x, y), (x', y')$ der nach 5.1.5 aus $\mathfrak{D}'$ entstehenden normalen Ebene Π .

Die Abbildung $\varphi: (x,y) \mapsto x$ von Π nach Π' ist offenbar ein Epimorphismus, für den zwei Punkte bzw. Geraden genau dann dasselbe Bild haben, wenn sie in der Relation $\circ$ stehen (für Geraden bezeichnet $\circ$ die nach 2.2.5 erzeugte Relation). Π' ist eine normale Ebene nach 5.1.5 und genau dann sogar Blockplan, wenn $\mathfrak{D}$ maximal ist.

Es bleibt zu zeigen, daß φ regulär und abgeschlossen ist. Sei $(x,y) \circ (x',y')$, also $x=x'$. Falls $y \neq y'$, sind diese Punkte unverbindbar; denn sonst würde etwa gelten

$$(x,y), (x,y') \in D_{ij} + (u,v),$$

also für geeignete Indizes $x = d_{im} + u = d_{in} + u$ und $y = a_{mj} + v, y' = a_{nj} + v$, woraus $m=n$ und somit $y=y'$ folgt. Widerspruch! Folglich ist φ nach 4.1.2 regulär.

Es bleibt nach 4.1.3.(ii) zu zeigen, daß φ (4.1) und (4.2) erfüllt. (4.1) gilt nach Definition von φ . Sei also $[(x,y), (x',y')] = 0$. Zu zeigen ist noch, daß daraus - falls $x \neq x'$ gilt - $[x, x'] = 0$ folgt. Angenommen, x und x' sind verbindbar, etwa durch $D_i + u$, z.B. $x = d_{il} + u, x' = d_{im} + u$. Es folgt $x - x' = d_{il} - d_{im}$. Nach dem bereits für den Nachweis von (5.7) Gezeigten gibt es dann einen Index j mit

$$(x - x', y - y') = (d_{il}, a_{lj}) - (d_{im}, a_{mj}).$$

Es folgt $(x,y), (x',y') \in D_{ij} + (x - d_{il}, y - a_{lj})$. Widerspruch! Also ist φ auch abgeschlossen und (Π, Π', φ) eine NTD-Ebene. Daß Π bzgl. $\mathfrak{G}$ regulär ist und die angegebenen Parameter besitzt, ist trivial.

' $\Leftarrow$ '

Sei umgekehrt Π eine bzgl. $\mathfrak{G}$ reguläre $(t, k-1)$ -NTD-Ebene. Dann ist Π , falls Π' eine (v, k, s) -Ebene ist (man beachte, daß in Π' jede Gerade k Punkte haben muß, da dies in Π gilt und der Epimorphismus von Π nach Π' regulär ist und wegen seiner Abgeschlossenheit (4.1) erfüllt), Π eine (vt, k, st) -Ebene: Π hat nach 4.1.4 offenbar vt Punkte; Π' hat $b = \frac{vr}{k} = vs$ Geraden, also hat Π nach 4.1.4 offenbar

t^2 vs Geraden, woraus sich nach 5.1.2 als letzter Parameter von Π st ergibt. Nach 5.1.5 erhalten wir also eine (tv, k, st) -Differenzenfamilie über $\mathfrak{G}$. Ferner induziert Π' wegen 5.2.6 nach 5.1.5 offenbar eine (v, k, s) -Differenzenfamilie in $\mathfrak{g}$. Wir können annehmen, daß $\mathfrak{D}$ und $\mathfrak{D}'$ wie in der Behauptung angegeben beschrieben sind. Wir setzen dann $A := (a_{ij})$ ($i=1, \dots, s$ und $j=1, \dots, t$) und zeigen, daß A eine $(t, k-1)$ -Differenzenmatrix (über $\mathfrak{R}$) ist. Wir betrachten etwa die Zeilen i und i' ($i \neq i'$, $i, i' = 1, \dots, k$). Die Punkte d_{1i} und $d_{1i'}$, von Π' sind verbunden, nämlich durch D_1 . Da Π eine TD-Ebene ist, sind also nach (4.2) auch $(d_{1i}, 0)$ und $(d_{1i'}, x)$ ($x \in \mathfrak{R}$ beliebig) verbunden, etwa durch $D_{1j} + (0, u)$. Dann folgt etwa $a_{ij} + u = 0$ und $a_{i'j} + u = x$, also $x = a_{i'j} - a_{ij}$. Folglich enthält die Differenz der Zeilen i und i' von A tatsächlich jedes Element von $\mathfrak{R}$ (genau einmal), d.h. A ist eine Differenzenmatrix.

5.2.8 Korollar

t und k mit $k \geq 2$ seien natürliche Zahlen. Dann sind die folgenden Aussagen äquivalent:

- (i) Es gibt eine (t, k) -Differenzenmatrix.
- (ii) Es gibt eine reguläre Menge von $k-1$ paarweise orthogonalen lateinischen Quadraten der Ordnung t .
- (iii) Es gibt ein reguläres $(t, k+1)$ -TD.
- (iv) Es gibt eine reguläre (t, k) -NTD-Ebene.
- (v) Es gibt eine reguläre (t, k) -BDTD-Ebene.

Beweis:

- (i) $\Leftrightarrow$ (ii): 3.2.7.
- (i) $\Leftrightarrow$ (iii): 3.3.2.
- (i) $\Leftrightarrow$ (iv): Folgt aus 5.2.7, da aufgrund des Dirichlet-schen Reihensatzes (siehe z.B. A.AIGNER 1975, Satz 102) stets (sogar maximale) (v, k) -Differenzenfamilien nach 5.1.7.(iv) existieren.
- (i) $\Leftrightarrow$ (v): ebenso.

5.2.9 Satz

Es gebe maximale (v,k) - und (t,k) -Differenzenfamilien über $\mathcal{G}$ bzw. $\mathcal{N}$ und eine $(t,k-1,\mathcal{N})$ -Differenzenmatrix. Dann gibt es auch eine maximale (tv,k) -Differenzenfamilie über $\mathcal{G} := \mathcal{G} \oplus \mathcal{N}$.

Beweis:

Wir übernehmen die Bezeichnungen aus 5.2.7 und bilden - wie dort beschrieben - eine (tv,k) -Differenzenfamilie $\mathfrak{D}'$. Da die (v,k) -Differenzenfamilie $\mathfrak{D}$ als maximal vorausgesetzt ist, ist jedes $x \in \mathcal{G}$ mit $x \neq 0$ darstellbar (als Differenz aus $\mathfrak{D}$), also nach dem Beweis von 5.2.7 (Nachweis von (5.7) für $\mathfrak{D}'$) jedes $(x,y) \in \mathcal{G}$ mit $x \neq 0$ als Differenz aus $\mathfrak{D}'$ darstellbar. Dagegen ist kein Element der Form $(0,y)$ darstellbar.

Sei nun $\mathfrak{D}''$ die gegebene maximale (t,k) -Differenzenfamilie, etwa $\mathfrak{D}'' = \{D_i'' : i=1, \dots, s\}$ ($s := \frac{t-1}{k(k-1)}$) mit

$D_i'' = \{(d_{i1}'', \dots, d_{ik}'')\}$. Wir fügen zu den Mengen in $\mathfrak{D}'$ die Mengen

$$\bar{D}_i := \{(0, d_{i1}''), \dots, (0, d_{ik}'')\} \quad (i=1, \dots, s)$$

hinzu und erhalten offensichtlich eine maximale (tv,k) -Differenzenfamilie über $\mathcal{G}$.

5.2.10 Korollar

q sei Primzahlpotenz und es gebe eine (q^2+q+1, q) -Differenzenmatrix über $\mathbb{Z}_t$ mit $t := q^2+q+1$. Dann gibt es normale Blockpläne mit den Parametern $k=q+1$ und $v=t^n$ für jede natürliche Zahl n .

Beweis:

Das folgt aus 5.2.9 mit 5.1.7.(i) und 5.1.5.

5.2.11 Beispiele

5.2.10 beinhaltet 5.2.2 (falls auch $q+1$ Primzahlpotenz ist, gibt es nämlich nach 3.4.10 eine $(t, q, \mathbb{Z}_t)$ -Differenzenmatrix); es ergeben sich also alle Beispiele aus 5.2.3,

aber noch weitere: die benötigte Differenzenmatrix existiert immer, wenn q^2+q+1 eine Primzahl ist, wozu $q+1$ nicht notwendig eine Primzahlpotenz sein muß, wie etwa die Beispiele $q=5$ oder $q=17$ (also $t=31$ bzw. $t=307$) zeigen. Soweit uns bekannt, sind die Beispiele von 5.2.2 und 5.2.11 normale Blockpläne mit neuen Parametern.

5.2.12 Korollar

k sei eine beliebige natürliche Zahl ≥ 3 . Dann gibt es normale Blockpläne mit Parametern k und v für jedes v , für das sämtliche Faktoren der Primpotenzzerlegung hinreichend groß (z.B. $> e^{k^2} k^{2k}$) und $\equiv 1 \pmod{k(k-1)}$ sind.

Beweis:

Das folgt unmittelbar aus 5.2.9 mit 5.1.7.(iv) und 5.1.5 unter Beachtung von 3.4.5.

Es gelten zur Diskussion nach 5.2.4 analoge Bemerkungen.

6. LITERATURVERZEICHNIS

=====

AIGNER, Alexander

- 1975 Zahlentheorie
 Walter de Gruyter, Berlin-New York

ARTIN, Emil

- 1957 Geometric Algebra
 Interscience Publishers, Inc., New York

ARTMANN, Benno

- 1971 Existenz und projektive Limiten von Hjelmslev-
 Ebenen n-ter Stufe
 Atti convegno geom. combinat. appl. Perugia 1970,
 p. 27-41

BACHMANN, Friedrich

- 1973 Aufbau der Geometrie aus dem Spiegelungsbegriff
 2. Auflage
 Springer-Verlag, Berlin-Heidelberg-New York

BAUMERT, Leonard D.

- 1971 Cyclic Difference Sets
 Springer-Verlag, Berlin-Heidelberg-New York

BOSE, R.C.

- 1938 On the application of properties of Galois fields
 to the problem of construction of hypergraecolatin
 squares
 Sankhyā 3, p. 328-338
- 1939 On the construction of balanced incomplete block
 designs
 Ann. Eugenics 9, p. 353-399
- 1942 An affine analogue of Singer's theorem
 J. Ind. Math. Soc. 6, p. 1-15

BOSE, R.C. | SHRIKHANDE, S.S.

- 1959 On the falsity of Euler's conjecture about the
 non-existence of two orthogonal Latin squares of
 order $4t+2$
 Proc. Nat. Acad. Sci. USA 45, p. 734-737

- 1960 On the construction of sets of mutually orthogonal Latin squares and the falsity of a conjecture of Euler
Trans. Amer. Math. Soc. 95, p. 191-209

BOSE, R.C. | SHRIKHANDE, S.S. | PARKER, E.T.

- 1960 Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture
Canad. J. Math. 12, p. 189-203

BRUCK, R.H.

- 1951 Finite Nets I. Numerical invariants
Canad. J. Math. 3, p. 94-107
1963 Finite Nets II. Uniqueness and imbedding
Pac. J. Math. 13, p. 421-457

CHOWLA, S. | ERDÖS, P. | STRAUS, E.G.

- 1960 On the maximal number of pairwise orthogonal Latin squares of a given order
Can. J. Math. 12, p. 204-208

CORSI, G.

- 1964 Sui sistemi minimi di assiomi atti a definire un piano grafico finito
Rendic. Sem. Mat. Padova 34, p. 160-175

DEMBOWSKI, Peter

- 1968 Finite Geometries
Springer-Verlag, Berlin-Heidelberg-New York
1970 Kombinatorik
Bibliographisches Institut, Mannheim-Wien-Zürich

DENES, J. | KEEDWELL, A.D.

- 1974 Latin squares and their applications
The English Universities Press, London

DRAKE, David A.

- 1975 More new integer pairs for finite Hjelmslev planes
Preprint No. 191, Technische Hochschule Darmstadt

DRAKE, David A. | LENZ, Hanfried

- 1976 Finite Klingenberg planes
 erscheint (Abh. Math. Sem. Hamburg)

HALL, Marshall Jr.

- 1959 The theory of groups
 The Macmillan Company, New York
- 1967 Combinatorial Theory
 Blaisdell Publishing Co., Waltham-Toronto-London

HANANI, Haim

- 1974 On transversal designs
 in: Combinatorics.
 Mathematical Centre Tracts 55, p. 42-52, Amsterdam
- 1975 Balanced incomplete block designs and related designs
 discr. math. 11, p. 255-369

HOFFMANN, A.J.

- 1952 Cyclic affine planes
 Canad. J. Math. 4, p. 295-301

HUGHES, D.R. | PIPER, Fred C.

- 1973 Projective planes
 Springer-Verlag, New York-Heidelberg-Berlin

JUNGNICKEL, Dieter

- 1975 Klingenberg and Hjelmslev planes
 Diplomarbeit, Freie Universität Berlin

KLEIN, Felix

- 1908 Elementarmathematik vom höheren Standpunkte aus II.
 Geometrie
 Springer-Verlag, Berlin-Heidelberg (3. Auflage 1925,
 Nachdruck 1968)

KLEINFELD, Erwin

- 1959 Finite Hjelmslev planes
 Ill. J. Math. 3, p. 403-407

KLINGENBERG, Wilhelm

- 1954 Projektive und affine Ebenen mit Nachbarelementen
Math. Z. 60, p. 384-406
- 1955 Desarguessche Ebenen mit Nachbarelementen
Abh. Math. Sem. Hamburg 19, p. 158-175
- 1956 Projektive Geometrien mit Homomorphismus
Math. Ann. 132, p. 180-200

LENZ, Hanfried

- 1965 Vorlesungen über projektive Geometrie
Akademische Verlagsgesellschaft, Leipzig
- 1975 Grundlagen der Elementarmathematik
3. Auflage
VEB Deutscher Verlag der Wissenschaften, Berlin

LENZ, Hanfried | JUNGnickel, Dieter

- 1976 Homomorphisms of partial planes and related
mappings
Manuskript

LINT, Jacobus H. van

- 1974 Combinatorial Theory Seminar Eindhoven University
of Technology
Springer-Verlag, Berlin-Heidelberg-New York

LÜNEBURG, Heinz

- 1971 Kombinatorik
Birkhäuser-Verlag, Basel-Stuttgart
- 1973 Einführung in die Algebra
Springer-Verlag, Berlin-Heidelberg-New York

MC NEISH, H.F.

- 1922 Euler squares
Ann. Math. 23, p. 221-227

PICKERT, Günter

- 1955 Projektive Ebenen
Springer-Verlag, Berlin-Heidelberg-New York

RYSER, Herbert J.

1963 Combinatorial Mathematics
Wiley, New York

SINGER, J.

1938 A theorem in finite projective geometry and some
applications to number theory
Trans. Amer. Math. Soc. 43, p. 377-385

TARRY, G.

1902 Le probleme de 36 officiers
C.R.Assoc. Franc. Avanc. Sci. Nat. 2, p. 170-203

WAERDEN, B.L. van der

1971 Algebra I (8. Auflage)
Springer-Verlag, Berlin-Heidelberg-New York

WIELANDT, Helmut

1968 Finite permutation groups
Academic press, New York-London

WILSON, R.M.

1972 Cyclotomy and difference families in elementary
abelian groups
J. Number Theory 4, p. 17-47

1974a Concerning the number of mutually orthogonal Latin
squares
discr. math. 9, p. 181-198

1974b Construction and uses of pairwise balanced designs
in: Combinatorics
Mathematical Centre Tracts 55, p. 18-41, Amsterdam

1974c A few more squares
Proc. 5th Southeastern Conf. on Combinatorics,
Graph Theory and Computing

1975 An existence theory for pairwise balanced designs
III: Proof of the existence conjectures
J. Comb. Th. (A) 18, p. 71-79

Lebenslauf

=====

Am 20. März 1952 wurde ich, Dieter Heinz Jungnickel, als Sohn des Buchhalters Heinz Jungnickel und seiner Ehefrau Ilse (geb. Beier) in Berlin geboren. Nach der Scheidung meiner Eltern im Februar 1956 wurde meiner Mutter das Sorgerecht übertragen.

Im April 1958 kam ich in die Evangelische Schule Steglitz, die ich im März 1962 wieder verließ, um das Gymnasium Steglitz zu besuchen. Im Januar 1971 habe ich dort das Abitur abgelegt.

Vom Sommersemester 1971 bis zum Sommersemester 1975 habe ich an der Freien Universität Berlin Mathematik und Physik studiert. Im Herbst 1971 wurde ich aufgrund eines Bundes-sieges im ersten Bundeswettbewerb Mathematik (1970/71) in die Studienstiftung des Deutschen Volkes aufgenommen. Im Mai 1973 habe ich das Vordiplom mit 'sehr gut' abgelegt. Während des Wintersemesters 1973/74 konnte ich dank eines Auslandsstipendiums der Studienstiftung in London studieren (University College und Westfield College). Im Februar 1975 habe ich das Diplom mit 'sehr gut' abgelegt. Mein Haupt-arbeitsgebiet ist (endliche) Geometrie (Diplomarbeit über 'Klingenberg and Hjelmslev planes').

Seit Juni 1975 bin ich als wissenschaftlicher Assistent an der Freien Universität Berlin tätig, wo ich schon zuvor (seit April 1974) als studentischer Tutor beschäftigt war. Seit 1972 habe ich auch insgesamt etwa 2 Jahre aushilfsweise an meiner früheren Schule (Gymnasium Steglitz) Mathematik und Physik unterrichtet.

